VOLUME 4

HACKING

17 MOST DANGEROUS HACKING ATTACKS

ALEX WAGNER

HACKING
17 Most Dangerous Hacking Attacks

Volume 4

by

ALEX WAGNER

Copyright

All rights reserved. No part of this book may be reproduced in any form or by any electronic, print or mechanical means, including information storage and retrieval systems, without permission in writing from the publisher.

Copyright © 2017 Alex Wagner

Disclaimer

This Book is produced with the goal of providing information that is as accurate and reliable as possible. Regardless, purchasing this Book can be seen as consent to the fact that both the publisher and the author of this book are in no way experts on the topics discussed within and that any recommendations or suggestions that are made herein are for entertainment purposes only.

Professionals should be consulted as needed before undertaking any of the action endorsed herein.

Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

This declaration is deemed fair and valid by both the American Bar Association and the Committee of Publishers Association and is legally binding throughout the United States.

The information in the following pages is broadly considered to be a truthful and accurate account of facts and as such any inattention, use or misuse of the information in question by the reader will render any resulting actions solely under their purview. There are no scenarios in which the publisher or the original author of this work can be in any fashion deemed liable for any hardship or damages that may befall the reader or anyone else after undertaking information described herein.

Additionally, the information in the following pages is intended only for informational purposes and should thus be thought of as universal. As befitting its nature, it is presented without assurance regarding its prolonged validity or interim quality. Trademarks that are mentioned are done without written consent and can in no way be considered an endorsement from the trademark holder.

Table of Contents

Introduction

Chapter 1 – Adware / Spyware / Malware

Chapter 2 – Man in the Middle

Chapter 3 – ARP Poisoning

Chapter 4 – Wireless attacks

Chapter 5 – Phishing, Vishing, Whaling

Chapter 6 – Password Cracking

Chapter 7 – Spoofing

Chapter 8 - Spamming

Chapter 9 – Xmas Tree Attack

Chapter 10 – Botnet

Chapter 11 – SQL Injection

Chapter 12 - Distributed Denial of Service

Chapter 13 – Worms &Virus types

Chapter 14 – Logic Bombs

Chapter 15 – Backdoors & Trojans

Chapter 16 – Ransomware

Chapter 17 – WannaCry

Introduction

Congratulations on purchasing this book and thank you for doing so.

This book is designed to focus on the most common hacking methods exist today. You will be exposed to how the most dangerous attacks are implemented using multiple methods.

If you are thinking of becoming an Ethical Hacker, also known as Penetration tester, the concepts explained in this book will provide an excellent learning opportunity that you can use in real life. The contents in this book are explained in everyday English to help you grasp these concepts faster. All through this book is designed to explain the techniques, Volume 2, and Volume 3 is focusing more on step by step implementation process. I have demonstrated 90% of hacking techniques in Volume 2 and Volume 3 step by step, using multiple operating systems and several software for the purpose of helping you learn how to implement certain commands in order to successfully gain power over any network.

If you are only interested in knowing how hacking works and how it is carried out, this book will be beneficial to you. For those who are only seeking to understand the theory behind hacking attacks, this book will also help you. In order to become an Ethical Hacker, you must understand first the why hackers and cybercriminals are operating in such large scale.

It is vital to understand how certain hacking methods are done in order to avoid become a victim yourself. This book will help you get ready against hackers and the most dangerous hacking attacks exist in our current world.

There are plenty of books on this subject in the market, thanks again for choosing this one! Every effort was made to ensure the book is riddled with as much useful information as possible. Please enjoy!

Chapter 1 – Adware / Spyware / Malware

Malware

First I will begin to tell you that most probably you will find Malware on Windows operating systems because most operating systems out there in a production environment are indeed some Windows based operating systems. When you think a hacker point of view, there is no sense to create malware for operating systems that only take 30% of the world's operating systems. Instead, the ones that are most common should be infected.

There are many different types of Malware out there, so I will begin to explain some of them, however first let me list the most common types for your reference.

- Adware
- Worms
- Viruses

- Spyware
- Trojan Horse
- Botnet
- Rootkit
- Backdoor
- Logic bomb

As you see there are so many different types of Malware that are often difficult to identify what type of Malware you might get infected.

The reality is that some of the Malware might be working together and then it would be even harder to remove them from your computer.

An example would be that you get infected with a Trojan Horse. However, while you would get busy to remove it, in the meanwhile, there would be an additional Backdoor that would get installed on another machine automatically.

What happens in such situation is that you might believe that you have removed every malicious software from your PC, however in the meanwhile, another software would install itself that would re-infect your PC once again. Sometimes they might be working together, and once you would delete a certain malicious file, it would trigger another file to re-infect your PC.

You could potentially get infected by simply browsing the web, and clicking on something that shouldn't, these might be an advert of some sort, but it can also come from a genuine website. Another form might be that you have received an e-mail and sometimes by opening the email without even clicking on anything can cause an installation of malware. Some of the e-mails would ask you to follow individual links to provide your opinion on a certain product or website, these all can trigger a malware that is very malicious.

From personal experience, I had once a malware that was an Adware, and pretty much any website I have opened, I kept on getting pop

advertisements. Anytime I have deleted all the software that wasn't from a genuine source, I have realized that after a while they all re-appeared with the same date of installation, even I didn't even touch my computer.

Malware exists for the purpose of financial gain, and some of the types are written for the only purpose of stealing credit card details, usernames, and Passwords.

Advertising windows can also make money for hackers in the way of being an affiliate for a particular product, and they would get a percentage of you, or anyone would buy those simply from does who would use those links that are kept on popping up on your screen.

Some of these advertising pop-ups might be visible already on your screen even right after you would open a web browser, and that would be an adamant indication that you have some malware on your computer.

Malware would use many methods. However the most common are to look for known vulnerabilities of an older version of operating system or the previous version of the application.

To avoid malware from targeting your computer, you must make sure that you are always running the latest operating systems available. Additionally, the applications that you have on your PC all must always be up to date with the most recent upgrade.

Adware

This is easily recognized as your computer screen would be full of advertisements that literally would become so annoying that they would drive you crazy.

If you are aware of Adware by experienced these types of issues in the past, you would know that it's one of the worst out there and the reason for that is so difficult to remove it that you just cannot be sure how to do so.

When you have an Adware on your computer, you would be able to recognize it by situations such as by only reading your favorite blog, then all of a sudden multiple ads would pop up on your screen. Mostly

advertisements and those are not necessarily the ones that you would be interested, so as I mentioned they are very annoying.

The primary purpose could many other thinks. Other than advertising only, and some of the Adware-s might be working with other malware that is logging all the information that you are accessing, every website you visiting, possibly logging all the usernames and passwords too and all those information would be redirected and routed back to the hacker.

Regards to performance issues, it's very common that multitasking such as opening multiple websites would slow down a bit, and often wouldn't even work, and your CPU would be spiking and would be continuously above 70%.

In some situation, you could even experience that your machine is irresponsive and looks like it's frozen. Some of the events could cause to damage your CPU (Central Processing Unit) so poorly that it could be critical.

In case you are unable to click on anything your best bet is to go ahead and open task manager, by using the combined keystrokes Ctrl + Alt + Delete

and choose the Task Manager from there.

Once you open your Task Manager, first check the user's Tab, making sure there are no other users remotely connected. Then test the CPU utilization in the Performance window, and see If your CPU is only spiking sometimes or it’s continuously high.

Sure if you are multitasking you will have higher CPU utilization then if your computer is only in a standby mode, however, I am sure that you would suspect if there are significant performance issues with your machine. It also depends on what other software are running in the background and how much RAM you have on your computer, as well how much RAM Is currently used and so on.

In case you believe that your CPU is indeed highly utilized, your next move should be to go on the tab called: Processes, and begin to analyze by sorting them as the highest CPU used, and to achieve that just click on the tab CPU. Then you should be able to see what processes are using the most CPU on your computer.

Any of the processes that are not familiar with you can right click and select properties for further understanding of what Corporation has created them.

However, if you see that some them are just taking too much of your CPU, you should shut down the applications by selecting them then click on End Task. Another way to close unwanted processes is by right-clicking on them and select End Task. I can tell you from experience that often to shut down Adware processes this is the only way to End them before it would take down your computer completely.

Once when I have been multitasking by opening multiple websites, after few minutes on each site I had numerous advertisements started to pop up, then I have left my laptop up and running for so long that Adware process was spiking the CPU for so long that turned my Laptop off. When I have

tried to turn it back on it was useless, so I had to install a new operating system to use that laptop again.

My last advice if you experience an Adware, and your computer is suffering from using too much of CPU, you should turn off your computer before it's too late. Next, hopefully, you will be still able to turn back on then try to save all your important document to an external hard drive, and install a new operating system.

Unfortunately, there is no guaranty that your files will not be infected, especially if you had a rootkit format of malware installed previously, however, to save your computer's CPU from potential damages new operating systems that I would recommend. You might be able to download an excellent anti-virus, such as Kaspersky of Norton, however often these Antivirus software wouldn't help as much as you would expect. Also, you must understand that some form of Adware might have been written in another combined form. Once you would try to remove the malware, the malicious software would react by activating another piece of software that would pop up on your screen and then would pretend to be an Anti-Malware or some Anti-Virus that would be able to remove all the Adware from your computer. Now you have to be careful as this is another method that hackers would use, that is to make you pay for an Anti-virus that would not remove anything, in fact, while you would install this so called Anti-virus, what you would be doing is installing another malware that would continuously infect your computer.

Recommended Antivirus Software is:

- Kaspersky
- Symantec
- McAfee
- Norton

- ESET

Spyware

This is another malware, yet this type of software is designed mainly to spy on computers.

To fully understand the reason why these types of Malware is so dangerous, I will begin saying the most common effects when dealing with Spyware.

First spyware could very likely be operating on your computer like Adware, meaning lots of advertisements. However, these types of ads would be popups that you might be interested in purchasing. What hackers would do is try to advertise an individual product to you from the third party with a hope of you as a victim would buy, and they would be getting an affiliate commission from each of those purchases. To narrow down your interest and understand your buying habits they would begin to spy on you, by monitoring your activities daily. For monitoring purposes, you would find that most Spywares have keyloggers built into them. Keyloggers log everything that you type into your computer even if you are not online. I mean everything, so let me give you an example:

Let's assume that you would write something like Hi John! Then you would backspace John and change it to Jack > it would be visible too. Keyloggers log every keystroke that you type, even if it’s a mistake that you correct

without saving the file, and that would be online web browsing, emails, Facebook messages, or offline word document, notepad you name it.

All those details would be transferred to another software that would analyze and understand your interest and start to advertise certain products to you.

You would never realize that someone was logging all your information, as well you would never know that has been sold on the internet, it's happening day and night all the time. To get spyware to your computer, you might be downloading a free software that has been written with the intention of installing spyware on computers.

The actual software could have been designed as a genuine free software, however, if the hackers would realize millions of people would download it, they would infect it with spyware and then re-upload it on a similar website. Victims then begin to download it, and all through the software would work just fine, however, while the installation takes place, additionally, you would be installing a spyware too, that would begin to act maliciously on your computer. The same method would apply for:

- free movies,
- free music,
- free pictures,
- free operating systems,
- free software and so on.

They all could have a hidden unwanted spyware inside, as hackers would know that millions of people are downloading such products all the time.

If you are good with math you should be able to understand; this would be a good business for them, of course, this is illegal. Therefore I would recommend you to stay away from unlawful activities.

This criminal activity is known as Affiliate fraud, and many large Cyber Criminal Organizations are operating as their primary income.

As you can see Malware types are dangerous as they would win against many victims one way or another. They would keep on advertising products and make money off you. If not they would try to manipulate you into buying fake antiviruses, they might do a Ransomware (more on this in a later chapter) with a locked screen and demand payment, or if you don't want to participate, then they would just destroy your operating system, then your computer eventually.

Either way, the end goal is always financial gain, and believe me, malware is not designed for some people, instead as many as possible. Spyware itself is the one that specifically designed to go after your money, either your Credit Card or Bank account information so that it can be sold on the dark web. Worse is that hackers would use your Bank account information and take money out of your account.

Protection against Man in the Middle attack

To do something against a Man in the Middle if you have one or two computers, you should make sure that you have an excellent antivirus. Preferably one of those I have mentioned in Chapter 1, however, you must make sure that your Antivirus is up to date every day, perhaps configure it by having auto-updates. Therefore once the Anti-virus company would come up with the latest upgrade, you would have a chance for more protection against bad guys.

Chapter 2 – Man in the Middle

Man in the middle indeed what the name implies, therefore someone would be sitting and listening to the source and the destination while traffic flow would be generated.

Additionally listening and capturing traffic, the man in the middle can copy and save all the traffic, then all that can be replayed and analyzed in more depth.

In Volume 2 I have explained in greater details the reasons why implementing and becoming a Man in the Middle is beneficial for Ethical Hackers as well Security Engineers, however, if you have not gone through that book yet, I would highly advise you to do so to get the most out of this book.

A quick recap on that subject was an example that you as Security Engineer might have to analyze a newly designed application, making sure it has no

vulnerabilities that can be exploited before it would be used in a Production Environment.

I have explained by using BurpSuite could be an excellent option that would not only be used to implement a Man in the Middle attack but analyze packets in more depth. As I mentioned, BurpSuite can be one of the best software for the purpose of monitoring and understanding exactly how a new Application would behave once in use. To have BurpSuite functioning, the only method would be to become a Man in the Middle.

Once you are a Man in the Middle, you are becoming the Endpoint to both, the source as well to the destination. Monitoring traffic flow in an authorized manner is very common amongst Security Engineers. However, there is a dark side to it too that I will now begin to explain.

Listening

The reality is that once there is a Man in the Middle between your laptop and your router, you might never even find out. That's scary. However, it's the sad true. Man in the Middle attack can be implemented in many different ways, and I have explained and applied the three most common ways that hackers could use against victims in the Book:

Volume 2 – 17 must-have tools every Hacker should have

By someone listening to your traffic could mean that everything you type in the computer could be recorded and analyzed in depth. Everything means your usernames and passwords to all websites you would visit, of course, the list of all those sites you would visit, anything you download from the internet or able to access, including all your Bank Details, all your social networking details, e-mails, and the list goes on.

Your data is very much considered a highly valued information to hackers and they would try to leverage on it in multiple ways.

Redirecting traffic

Black hat hackers can listen to your traffic flow in monitoring mode. However they would also try to redirect your traffic for affiliate frauds, so

your wouldn’t get the response that you meant to be, and many people would just believe that thinks have changed with a particular website as they not seem to appear as they used to be.

That’s right; once a Black Hat hacker would have gained enough information from your browsing habits, and find it that you do visit eBay 5-10 times a day, the Hacker would try to use some template and manipulate you to visit a fake eBay website. Taking it further, the Hacker with evil intention would be trying thinks like you forgot to purchase an individual Item, the one that got stuck in your browsing history, of might have been learned from your browsing habits. Then the Hacker would try to make you pay for an item on a fake website, using PayPal or other paying methods used over the Internet. Once you would be presented with the payment link after you would type your details, it wouldn’t work.

If you already know the reason why then congratulations! The answer is indeed to steal your PayPal information by what you would type into the fake PayPal link.

This time you don’t make any payment, however, the Hackers would have logged all the information already that would be enough for them to make any other real Payments on other platforms, but believe it or not, this is happening all the time, day and night all over the word in every minute. So the cherry on the top is that these type of hackers wouldn’t use your information to purchase items or products on the internet. Instead, they would sell them in batches on the dark web for an average price of 10x Units of Credit Card Details + passwords for the mean price of $5.

Sure the price is not always same, and if these Man in the middle attacks were implemented on a large Company’s systems, Black Hats would have full access to financial purchases that the Company would frequently participate, and once they would identify that, they would raise the price of the Black Market. Typically they would ask for a price in worth of dollars. However, they would ask to get paid in Bitcoin to be untraceable. Therefore they never would be found.

Redirected traffic might results as an affiliate fraud, so they would begin to make you advertising certain websites by manipulating into seeing ads that

you might be interested, and that's where they would introduce some malware, such as spyware.

Injecting payload into existing traffic:

Additionally, Blackhat Hackers would be able to insert the particular payload into the flow by changing some of the details of the traffic, and this could be implemented in both ways.

Some of these injecting methods might be changing the source details telling the destination that the address of origin should be the Hackers laptop. Therefore they would receive the answer first. The other way to implement these techniques is not touching the source details. However the destination details would be analyzed and changed, so the end users or victims would receive a different web page and not the one that they have asked for in the first place.

This could happen in many forms too, and hackers could be sending back to the source a fake web page that would ask you to download a fake JAVA application that required to proceed to the internet page.

Another way might be that you could be receiving a message similarly to JAVA application but this time it would be ADOBE reader upgrade would be required to proceed to the web page. The issue is that recognizing the exact upgrade requirements and the fake ones are tough. Therefore you might do a test by asking someone else if they would visit the same web page what would be the outcome. In case it's not the same, then you should be able to recognize that probably someone else is sitting between your computer and your destination.

Chapter 3 – ARP Poisoning

Man in the middle attack could come in many forms as I mentioned before but the most common implementation is ARP poisoning.

ARP Poisoning

To introduce the technique of ARP poisoning, you should understand the basics of ARP its purpose and how it functions, even not required to become an ARP expert the bare minimum is to know some basics

ARP stands for Address Resolution Protocol, the purpose of this protocol is to translate the IP Addresses to their MAC Addresses (Physical addresses) of all the networking devices that reside on the LAN (Local Are Network).

To implement this command on the Windows operating system, you may proceed by opening a command line interface and type arp –a

Finding the Command Line is easy, on any Windows Operating system click on Windows start menu, then in the search field type: Command Prompt and enter to launch it.

Next just type arp for further details:

As you see, there are few more options related to the arp command, using some of the variations such as:

- Arp – a > This would display the current ARP entries specifically on this network that this computer is aware of by listing both the IP Addresses as well the MAC addresses of those devices.

- Arp – d > Deletes the ARP entry for the host that we would specify.

- Arp – s > This command would help to add hosts and associate it with an IP Address.

- Arp – v > This command would display the current ARP entries in verbose mode and all invalid entries as well the loopback interface would be shown.

I am only trying to explain some basics and the variations as well some options are available with ARP. However, it's not a mandatory to know everything.

Instead, what you have to understand is that computers and networking devices on the same network would know each other by creating an ARP table, so they would reference that to locate each other on the network.

This is all great. However, hackers would take advantages of ARP tables by introducing themselves on the network with fake MAC Addresses making believe computers that they are the new Router. Therefore the real ARP table would be poisoned.

Once the ARP table would be poisoned by the Man in the Middle, the computer would believe that the new route to the internet would be a new address. Therefore, everything would go through the attacker.

I have demonstrated in few different ways on how to become a Man in the Middle using Back|Track or Kali Linux in Volume 2 and Volume 3 both using Wired and Wireless networks. Therefore I will not get into any more specifics. Man in the Middle attack can be achieved in many different ways. However the concepts are always the same, but then it's up to the attacker or penetration tester for what purposes this method is being used.

Chapter 4 – Wireless attacks

The reality is that there are so many different ways to attack wireless networks that I don't even know where to begin. I have dedicated a book specifically for implementing Wireless attacks in Volume 3 where I have dived into more details on how to use multiple methods regards to attacking Wireless Networks.

Most people love to use Free WIFI, in fact, any wireless networks as the technology expanded we don't need wires anymore. Now that the 21st Century began we all realized that Wireless networks are now everywhere and because more and more Access points all over the signals have grown dramatically, therefore we have started to use the Internet wirelessly. Furthermore, we have got to the point that we have begun chatting on our mobile devices, then shortly after we were able to do Skype calls and for a long time now we can stream live TV channels in HD quality.

Because wireless networks are in our everyday life, hackers have realized that too. Multiple techniques can be used to gain power over Wireless Networks.

At first Wireless networks were used as some backdoors by Hackers to get access to the leading network of individual companies. Even now that wireless networks are lots more secured, believe it or not, hackers still gain access through a Wireless Access Point as still many large organizations didn't take enough steps to implement proper security measurements around their Wireless Networks.

As I mentioned before we all love to use free WIFI Hotspots, but the sad true is that many of has no clue how big of a danger it might be once we would connect to a Rogue Access Point that advertises itself as a genuine Free WIFI Hotspot.

Rogue Access Point

To create a Rogue Access Point is very easy. Therefore big business must have many security measurements in place to protect the Wireless Network.

To duplicate a whole access point many people think that an average hacker should have to get an actual access point and configure that and place it somewhere, even this might be one way to go about it; nowadays there are more brilliant strategies for wireless hacking purposes. To become an Ethical Hacker, or a Security Consultant, you must understand every little wireless hacking method that is out there and the bad guys might use against you or your company that hires you. If you don't know what threats are out there, then you won't be able to implement the right security measurements. Therefore you will not be able to protect the network.

Most of the Access points are not consuming any electricity, and they are PoE devices, meaning Power over Ethernet is how they function. Therefore access points must be connected to something that would be powered on. Additionally, Access Points are not very small, so you will not see hackers walking around holding one in their hands. Instead of having an Access Point, you can virtualize one within your laptop using either Back|Track or Kali Linux. Once you have a laptop, you might proceed and install

Back|Track or Kali. However, you might just install it on a Virtual Machine and bridge it together with your notebook then began to hack any wireless network.

To become a Rogue Access Point on a Wireless Network, you can configure Back|Track or Kali to start to monitor Wireless signals, then analyze existing genuine Access Points in more detail. Next, you could learn the MAC Address of the valid access point and what channel it's using for wireless purposes. Having all that information, you can configure your Back|Track device to advertise the same details then become the new fake Access point aka Rogue Access Point.

Of course, there are many other configurations required such as DHCP services, DHCP Server settings to provide IP Addresses to the clients, or I should say, victims. Next would need to implement NAT Network Address Translation so that private Addresses would be able to get translated to Public IP Addresses, lastly routing functionality must be configured so that victims would be able to communicate and have access to the Internet.

Yes, you are right the victims would have access to the web through the Rogue Access Point. Therefore, it's also known as a Man in the Middle. I have explained and demonstrated these steps in Volume 3 in case you want to practice in your home lab environment. However, I wanted to provide a high-level overview what a Rogue Access Point could do.

Man in the Middle on Wireless

As I explained, once there is a Man in the Middle, Everything that you do, including every website you visit, every username and password you type can be logged by the Man in the Middle. Additionally, to be registered, your details can be modified, or even changed while you would fill some important inline document for someone it would be written by someone else and so on. I have discussed already what a Man in the Middle could mean, however yet I never explained that one of the most common ways that are used is indeed through wireless networks, by having victims to connect to a Rogue Access Point.

This is key to understand so next time when you see a free WIFI Hotspot; you must make sure that is the real genuine access point that advertises the real wireless network, as once you wouldn't want to connect to a Rogue Wireless Access Point.

Mis-Association Attacks

Another method I have demonstrated and successfully implemented in Volume 3 – Hacking Wireless Networks.

What you have to understand is that by using such operating systems like Kali Linux or Back|Track you can fake create your own MAC address, therefore you can become anyone that you choose to be. What I mean is that once you begin to monitor wireless signals with your Virtualized Kali Linux, then identify a Wireless Network, you can identify both the Access Point as well all the Clients that are currently associated with it. As I have mentioned before you might fake the Access point's MAC address and become a Rogue Wireless Access Point, however by analyzing the wireless signals you are also able to learn enough details about the clients too, to fake them. What you need is the MAC address of a trusted Client that already established a connection with the Access point. In case I am confusing you, please remember that every router or access point is remembering your devices MAC address and that's why you don't have to type the password each day when you are about to connect to a wireless network that you have provided a password previously. In fact, you don't even have to click or choose the SSID (Service Set Identification) as your device would find it, and join to it automatically.

As much as you know that fact, believe me, all the black hat hackers know that too, and they would easily exploit this vulnerability by using an OS (Operating system) such as Back|Track or Kali Linux. Again all you have to do is use a trusted device's MAC address and assign that to your own. Well by doing that you still have to get on the wireless network, therefore you have to send a de-authentication message through wireless signals to de-authenticate all the trusted clients. While they would try to re-authenticate

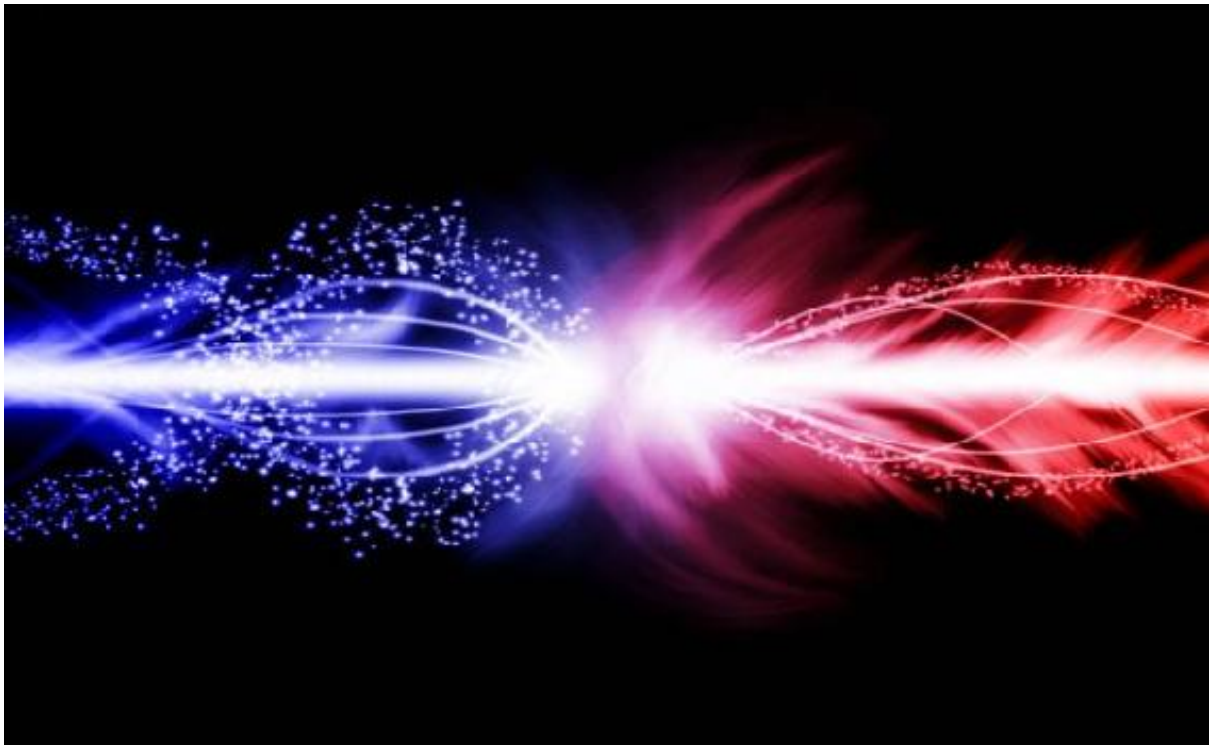
your device, they would gain power, and they would be connected already. To have your device connected faster than the actual device, you can do a little tweak by making your wireless signal stronger so that would help you get attached to any wireless network faster. In case you have doubt on how to implement such method, I have a step-by-step guide in Volume 3, specifically for Hacking Wireless Networks.

De-Authentication Attack

I have just explained why and how would a hacker plan up a Mis-Association Attack, and the purpose of that would be is to get authenticated on a wireless network that the hacker would want to exploit in same ways. Once you would join a network there are many thinks that you could do, and the hackers would not necessarily want to enjoy free WIFI, instead to something more sophisticated. Sure the majority of the hacking is for financial gain. However there are other factors too, that would be such as espionage, or it could also be impersonation and so on. Occasionally hackers plan would be only to cause a simply delay, or something that would slow down the network, or cause issues such as failure for individual devices to operate or connect to the network. As I mentioned before by Back|Track or Kali Linux you can monitor and learn all the MAC addresses of the real clients that are connected to the network. Once you would learn enough data of the clients, you could begin to run an automated de-authentication request for each of those trusted devices originating it from your Attacker laptop. Make it look like to the AP-s (Access Point) that the request was coming from the clients; the AP would de-authenticate them all, resulting the end-users to wonder why they have lost Internet access. Once it would be reported to the IT Department, engineers should have some time to analyze the logs and understand what exactly happened, and there would be nothing against the regular traffic flow, however, if everyone would be disconnected from the same wireless network that would cause suspicion. Still, it would be hard to find out what exactly happened and who was the villain in the first place.

Wireless Collision Attack

As I explained in Volume 3 – Wireless Hacking Book, Wireless Collision can be found everywhere, even if not always, however, other devices can cause Wireless collisions.



Such devices might be cordless phones, microwaves that could cause interference, therefore, could weaken the wireless signals.

Because wireless access points are sending signals to the air using certain channels, there is a chance that your neighbors could have wireless access points too that might use the same signals as your home router. Most of these access points would provide unyielding signal far as 30-50 meters in a precise radius. However, some could send out messages 200 – 400 meters if there is no interference and there is an obstruction.

Wireless signals would begin to decrease once should go through windows, doors, or walls, and thicker are the object weaker the wireless signal would become. This is common sense. However, most people don't think about possible interference issues, and the most common could be simply another Access point nearby that would use the same channel, therefore, would

cause wireless interference. The reality is that many people live in flats and they would have 3-5 neighbors very close, and most of them would have issues with the wireless network in their home. In the same time if they would check their wired network there would be no problem, however, due to the increasing number of wireless home networks, this is becoming a regular issue.

As I explained some of the fundamentals before you can configure both Back|Track and Kali Linux to provide a stronger signal, moreover you are also able to monitor wireless signals, and identify other wireless access points and what channel they use to operate. As you see, Hackers know facts too, and if they wish to cause an issue on an individual wireless network, all they have to do is configure their Back|Track box to use the same channels as the victims. And quickly the interference would become so high that on the victim's network could become so slow that would be useless, eventually would drop all packets, and every single client would lose network connectivity. Taking this further, hackers go far as installing a Kali operating system in a Raspberry Pie, and would hide it somewhere close to the targeted wireless access point, furthermore would even attach the Raspberry Pie to a Drone, and land it on a Building that would be their target. Once a sophisticated wireless collision attack would be implemented, it's possible to damage the Wireless access points so badly that would effect all SSID-s. Therefore, all the clients would drop off the network.

Wireless Replay attacks

This method has lost its fashion, however in the past was very much used and for some might become an old time favorite way to hack the wireless network. Therefore it's fair to explain the concepts.

As I mentioned before catching wireless signals are very easy, as they are everywhere, so before deciding what wireless network you would want to connect to, first, we would have to monitor the wireless signals. While monitoring the wireless traffic, we could record it by Wireshark, that would help for further analysis regards to what kind of communication is happening on the wireless network. Simply we would want to look for a

packet where a client would authenticate to a particular SSID. This packet would confirm the password required for logging on to the wireless network, and if you would use that to replay the very same message in the air, there is a possibility for the access point to authenticate you as a trusted device. The reality is that most large companies are now using new standards for better security. However, there are still many businesses could be exploited using this technique.

Protection against wireless attacks

As I mentioned big companies such as Banks or any other financial Organizations have now learned that Infrastructure security is essential, therefore most of them have good security in place such as ISE – Identity Services Engine, or at least ACS – Cisco Access Secure Control that is the old version of ISE.

Moreover to security, at least one vendor type of Firewall would be required, such as Cisco Systems, Checkpoint, Juniper, Palo Alto, Brocade and so on, however, most companies would rather having two different types or firewalls, just in case one would be compromised.

IDS - Intrusion Detection Systems also famous for wireless security to identify anomalies on the network, so that would fire up alerts in the system, then other devices such as IPS – Intrusion Prevention Systems would prevent such wireless attacks.

Regards to the WAP-s Wireless Access Points, most of them are PoE (Power over Ethernet) devices. Therefore they would be connected to network switches. On network switches additional commands would require being implemented too, in case someone would try to log in to the network using wired connection such devices like a Back|Track or Kali Linux.

Wireless network protection is critical, and if you have a personal wireless network at home, you probably using a protocol such as WPA-Personal or

WPA-PSK.

PSK stands for Pre-shared Key, and that would normally be your password. Therefore anyone who would want to connect to the wireless network would have to provide the same password. Unfortunately, PSK can be broken into as well, using Brute-force attack, or even Dictionary attack. Both Brute-force and dictionary attacks are relatively simple tasks to perform, as once you ready to implement them, the software would do the job and eventually would find the password. What I would suggest is to use a password that is very complex should include:

- Uppercase letters
- Lowercase letters
- Numbers
- Multiple symbols
- At least ten characters long
- Do not use dictionary words

I know that most people wouldn't bother much and use simple passwords such as password1, however more complex is your password, more challenging is to crack it, therefore here is an example that you could use if you want to stick to password1:

Try to sue something like Pa$$W0rd! > the o would be a zero of course, however, try to avoid anything that would be related to words like password or pass, furthermore anything that would be related to you, such as:

- your name,
- your details
- Any date of birth of yours or close family members
- Any names that are close family members

I am explaining these, because unfortunately still most people using similar passwords, words that they could remember easily. This is something the

bad guys would be aware too and using social networking sites; it is very easy to find out passwords related to people.

As I mentioned using Brute-force or Dictionary attacks, there is no escape even if cracking passwords could take days or weeks, eventually would be broken by many software.

This is one of the main reason Companies implementing password policies, such as password complexity, and additionally to be changed in every 30 days.

To be honest, in early 2017 there was a new software that was able to crack any password just below 30 days. Therefore the newly recommended password policy is 20days.

Again, I can tell you now that still many companies even aware of this information, still will take months or even years to implement the 20days password policy, as it's just too much of pain, and of course who likes to change their password in every 20 days. Before you think there is no way to do such thing, let me suggest something that you might consider regards to change your password even in every day if you would want to.

Think about dates, such as months, or the name of the days, then use those backward.

If it might be something that is too difficult to remember, and you want to use a single word, then use it three times. For example, you want to use a password like Pass123; you might use it as Pa$$123Pa$$123Pa$$123 > it's easy to remember and tough to crack.

As I mentioned before, please don't use this example or anything related to to the word: pass. However, you might find it helpful and able to apply it to your existing password I order to make harder to be cracked.

Chapter 5 – Phishing, Vishing, Whaling

Phishing

The word Phishing it does sound like fishing, and this is because the method is indeed very similar. A traditional fisher would typically throw the net into the water and wait for a catch. Wait until fishes, or I should say victims would be fool enough to be caught, and inevitably more fish would end up in the net, more the fishermen will happier be, moreover more net the fishermen uses bigger the chance to catch more fishes.

When it comes to Phishing, the techniques are similarly used. However, the most common form is via e-mail. What the so-called Phisher-men would do is send e-mail that would have an attachment, and being sound like an old friend, the message would contain something like:

, It's been a long time, and just remembered that you always wanted to see these files, and now I have attached it for you. Let me know your thoughts.''

Of course, there are many similarities like these, and the reality is that many people become a victim because of their curiosity by trying to open files from unknown sources.

If you were reading this book thinking there is no way that anyone would open attachments like this, believe me, you would be surprised how many people become a victim of Phishing attacks. Again we are humans, and we all thought differently, and we all have different reasons to make mistakes, both knowingly or unknowingly.

When the question approaches people: why did you click on the attachment? – Some may answer that they are waiting for some documents, some just too tired and clicking on any e-mail that's in the inbox, and of course, there are many of us just too curious.

Curiosity comes in many forms, and when humans get confronted of explaining or answering and being thoughtful, often people respond otherwise.

Let's take an example by asking ten people if want to see their manager's e-mails. Yes, they all would say that not interested, however, if the question is that no one would ever know that they had access to their manager's e-mails and they would answer anonymously the typical answer would be a different outcome.

As you see, some people when receiving a malicious e-mail addressed to their boss, by landing in their mailbox, they would be even more curious to see what the attachment contains.

Phishing comes in other forms too and the second most common would be a link attached to the e-mail. Again nothing new here, but attackers still use this technique by creating an emergency o such by writing something that victims would easily fall for. Some example could be:

- OMG! Check the link; there will be an earthquake!
- You were not going to believe it! Check What she did while she was naked!

The list could go on forever, and there are still people becoming a victim of Phishing attacks when they have a surprise.

Other forms of Phishing types that are more and more common is the ones would represent a known Authority. These would be fake e-mails look like from Banks, PayPal, eBay and such where the e-mails would contain something like:

, Hi, we have detected some unusual activities in your account. Can you please confirm your security details by clicking the following link.''

I have received one like this before from a Bank that I have never account with, so it was easy to eliminate. However, you have to understand that these attackers are fishing and sending the same e-mail to millions of people all the time. So the way they would be trying to scam you is the link would probably another fake website, frequently very similar to the one official site, and there would be some of the questions that you should be providing answers. Reasonable questions that the real company would ask too, but this times once you would submit the information, you would send your details to the bad guys. Situations when receiving e-mails from your Bank or your PayPal or any known legitimate authority, instead of following the link they sent you, you should go ahead and type the actual web page link. Next try to log on and see if you have received an e-mail from the company in question, instead of making a terrible mistake. Even if the link you would receive might be very similar to the genuine one, still my advice is to be cautious and don't become a victim of old style Phishing attack.

Vishing

Again another similar word to fishing and the reason for that is because the bad guys using similar method to phishing, however, this time they would do carry out over the phone. The word comes from Voice type phishing. Therefore, it's known as Vishing. You might have encountered such situation, however in case you not familiar with Vishing, then let elaborate on it with further detail. At the end of the day, this is for those bad guys that

are indeed good with their social engineering skill set, as once they call a possible victim their job is to convince you to trust them. What their goal is to make you believe that you can trust them. First, they would call and introduce themselves as they call from a known company or Bank, and so they would explain that your bank account might have been hacked, as there are some unusual online transactions have been taken place recently. Of course, some people already would get a heart attack, and because they would keep on insisting that they want to help you and make sure that your money has will be recovered, you should be helping them identify all the places that you have been shopping recently. However, before doing so, they would run a security check, making sure that they are indeed speaking to the right person, and not the thieves. Then they would begin asking you to provide some personal details. Such would be your security code in full. Then they would you're your mother maiden name, you address, and once they would have enough information, they would tell you to relax now, and they will take care of everything, as now your bank card is secured, and they will call you back shortly. These type of people scamming their victims over the phone all they long, unfortunately, they have the nerve to do so, and anyone falls for their scamming speech might suffer further consequences. However once the bad guys have enough information to purchase with, they would begin doing that, or either they would sell your online information places like the dark web.

I would advise that you do not provide all your details to anyone over the phone, even some bad guys can be pretty convincing, for your good, please do not fall for scammers.

With most Banks, they are helpful and might recover some of the money if not all that online thieves might take away from your account, however it might take some time for them to investigate all that, and you could go through a great pain. The largest organization like Banks would have a set of questions. However, you could also ask for some proof that they are indeed who they claim to be. You might ask such thinks like, if you have access to my bank details, then please tell me what dates do I pay my mortgage or water bills. If a person were really calling from a Bank, for example, they would have access to your Bank details so that they wouldn't ask for your Bank Card information, and even if they ask to provide your

online security digits, they probably ask for your third and last security number instead of all.

Other types of Vishing, for example, someone would call you from your ISP – Internet Service Provider. They would explaining that your router settings will be changed due to a hardware upgrade that they recently implemented. Therefore you must provide remote access to the ISP's engineer to set everything on your PC for continuous internet connection. Now again, if they say that they should be able to talk you through the process that would be your best option. However, I would recommend you do not follow everything they tell you as they would trick you into opening an individual page that could install a backdoor to your PC, or worse. You must make sure you have a full confirmation that they are really who they claim to be so that you wouldn't get into any trouble.

Smishing

SMS phishing is another form of vishing; an example is by receiving an SMS stating that you would be entitled to claim 2437 dollars from your Bank. The other famous claim is a Car Insurance, but the point is that the message would contain a link to click on to proceed with the claim or even a number that you should call. Again please do not be greedy, by thinking that you will get 2437 dollars for no reason just out of the blue. This types of scammers also have the same goal mindset, and that is to steal your information so they could profit from it one way or another. Hackers often use a technique that instead of sending a TXT message from a Random number, they would make it look like very legit by renaming the caller ID, for example, they would name XYZ Bank. This would give new trust for the receiver, however, to be even more believable, they would explain in the TXT to call a specific number. If you would call that number that has been provided, what you might find is that a very professional answering machine would be explaining the following:

Thank you for contacting XYZ Bank, we appreciate your patience; someone will be with you shortly, however, if you like to speak to someone now, please choose the following options:

- To speak to the Marketing Team, press 1,
- To speak to the Sales team, press 2,
- To speak to the IT Department, press 3,
- To speak to the COE, press 4
- To listen to these options again, press 5

And these would be in the loop of course, and to be honest doesn't matter what option you would choose, in the end, they would try to scam you one way or another. This is an IVR – Interactive Voice Response that would even provide additional credibility to the hackers by really doing their best faking a particular company.

Spear Phishing

The end goal nearly always the same when it comes to Phishing attacks, and that is your login details, such as usernames, passwords, Bank account details, so I can confidently say that the objective is some financial gain.

Using traditional Phishing methods, the bad guys have learned that using a broad net they may be able to catch some fishes, however, to be more successful, they should be more personalized, and go after one particular fish each time. When it comes to spearfishing, the e-mails are very similar to a Phishing attack. However the message would contain your first name,

and the rest of the content would be very close to your occupation, somehow related to your daily life or might be to your recent online purchases. Using my example, I normally get emails like that once or twice a week, and they always try to invite me to some expensive Microsoft training that I could be a part for free of charge if I would register by clicking on some ridiculously long link. Some others try to sell me some servers that are currently at a discounted price, but I should check their brochure for my reference that is attached.

They are trying their best and coming very close as they can. However I do not specialize in Microsoft, neither my hobby to buy servers, so I only block these senders, but I have to say that the e-mail structure and grammar is excellent, sometimes nearly convincing that they wrote some of those e-mails specifically to me. Again this is anther type of social engineering, trying to influence me by a personalized e-mail related to my everyday. Still, this is called Spear Phishing, nothing more. Hackers try to succeed in convincing you by personalized e-mail, they may even reference another friend name who you would know so you would think less in regards to trusting the sender or not. To succeed as a Spear Phisher, there is some research would require, and by those few minutes of researchers they could learn about you and your friends or colleges and using those similar terms and friends names in the e-mail. Indeed they can be very convincing.

The reality is that you could be able to spot some of the differences within the e-mail address or attachments that would just look odd, or some of the links that you shouldn’t click on can be very long, and you wouldn’t see any real English words in it. These are so well written, that even Mailing security servers, such as Mail Marshal wouldn’t catch them. In your Gmail, they would turn up in your inbox rather than in a spam folder. Therefore I would highly recommend that you double-check everything in such emails and do not click on any link or attachment that the e-mail may contain.

Whaling

Now that you have understood the core of Phishing as well a Spear Phishing attack consider this: Whaling! If you think about what the bad

guys have learned from all these types of attacks, is why should they proceed by traditional unsuccessful Phishing attacks.

Going after all those little fishes, with a small amount on their Bank account, if they could just go after one or two big fishes instead who would have probably more money on their Bank account, as well they would be more embarrassed if they would be hacked. In one sentence Whaling is Spear Phishing a big fish. Big fishes are like Company Directors, CEO-s CTO-s and so on, and going after someone who has potentially a higher authority is called Whaling. Again these type of people wouldn't open e-mails like traditional Phishing materials, however whaling attacks have recently increased in volume, and many of them are indeed has had success. Whaling would not necessarily mean that the real CEO would be hacked. However CEO-s do have personal assistants who answer telephone calls, schedules meetings, answering e-mails, organizing companies purchases, therefore looking after quotes, and invoices and much more. So as you see, some bad guys would exploit this vulnerability, and try to hack into the PA's (Personal Assistant) PC by implementing Vishing such as an ISP, or from an IT Helpdesk who want to check on the PC due to fixing of an earlier made a

mistake or such like that. Once the bad guys would have access to the PA-s computer, it would be very easy to gain further information about the actual CEO, that could be used against him or her. In case the hackers would go after specifically the COE, or an Executive, they would have to provide specific details to convince a highly ranked company Manager. Therefore the bad guys must be preparing to whale for longer than an average Phishing attack. When you think about Company Executives, have access to more details than anyone else, and the Hackers know that too, therefore you must understand that for Executives should have many other layers when it comes to Security. However, CEO-s are busy with the Business. Therefore IT Security must be providing continuous training to the Executives making sure they wouldn't make any mistake.

Chapter 6 – Password Cracking

There are so many different methods to hack certain systems. However one of the easiest ways is still with the right username and password. If I give you my username and password because I trust you, then you would log on using those should be legal, however also would be dumb of me. Some of you might be sharing your usernames and passwords with your boyfriend, girlfriend, wife or husband. However, I would suggest you NOT to for the following reason:

Imagine that your partner knows your Bank account number and your password. However, he or she would get hacked, and those details would be stolen then you would realize that someone is making purchases illegally. Would you blame your partner for not being careful? Or think if it happens exactly in the opposite and is you that has been hacked, and not only your credentials have been stolen, but your partners too, and you still have explained that you have not been careful enough… Either way, your username, and password should not be shared with anyone, preferably not written down anywhere, or saved anywhere, especially places or websites where it would be readily available to others.

I have explained in some previous chapters about strong passwords and requirements for them. Therefore I will not go into more details on that subject. Instead, I will begin to explain some of the most known variations of password attacks.

Dumpster diving

This is an old technique of going through the trash, having a goal in mind to find useful information. This can be messy, and dangerous work, as you never know what you mind find in the bin, however even today there are many people misplace certain information might have been printed by mistake or only temporary use. The reality is that people still write down usernames and passwords then throw them into the wrong bin. Most companies are practicing having a confidential bin, therefore, additionally, hackers could have so many other ways to find or crack passwords that this technique are indeed out of fashion. However since the 80's until the early years of the 21st Century, this has been very common for hackers.

Shoulder surfing

When you work in the office, there are almost always someone close by and could potentially see your password that you type into your computer.

You should always be aware of your surroundings, and look out for people around you are not watching what you type when your password would require. In case someone just keeps on watching you, wait until they would pay attention somewhere else. When I was still a Junior Engineer, I was working with a Senior Telecom Engineer, who loved to wind me up by cracking my passwords for fun. I wasn't happy about it. However it was always a good laugh, and I have learned from my mistakes. One day he showed me a video on his mobile phone that was played in super slow motion. The Video camera was focused on a keyboard, and I was able to see every single keystroke. Seeing after the fifth character I realized that is me on the video typing my password, looking to the direction of the angle of video might have been shot realized it was where he keeps his mobile cell phone on the charger. I was embarrassed, and certainly changed my password right then, but this time I have covered my hands so no one can see what I typed. The lesson for me and to everyone is that because you are a typing super fast and having an adamant password, means nothing is

someone can record it and replay in slow motion. Therefore you should look around no matter of your location where you may type your password into any device.

When I take public transport, and sometimes I get on the crowded train, it's unbelievable how many people log on to their Companies e-mail provider and so many people can see the password they type in as well the contents of their e-mails. I have a feeling too sometimes that covering my hands are so unethical, and many people feel embarrassed when they should do it, and unfortunately, many people just don't do it. However, the real embarrassment is to watch a video recorded you typing the password that is visible, believe me.

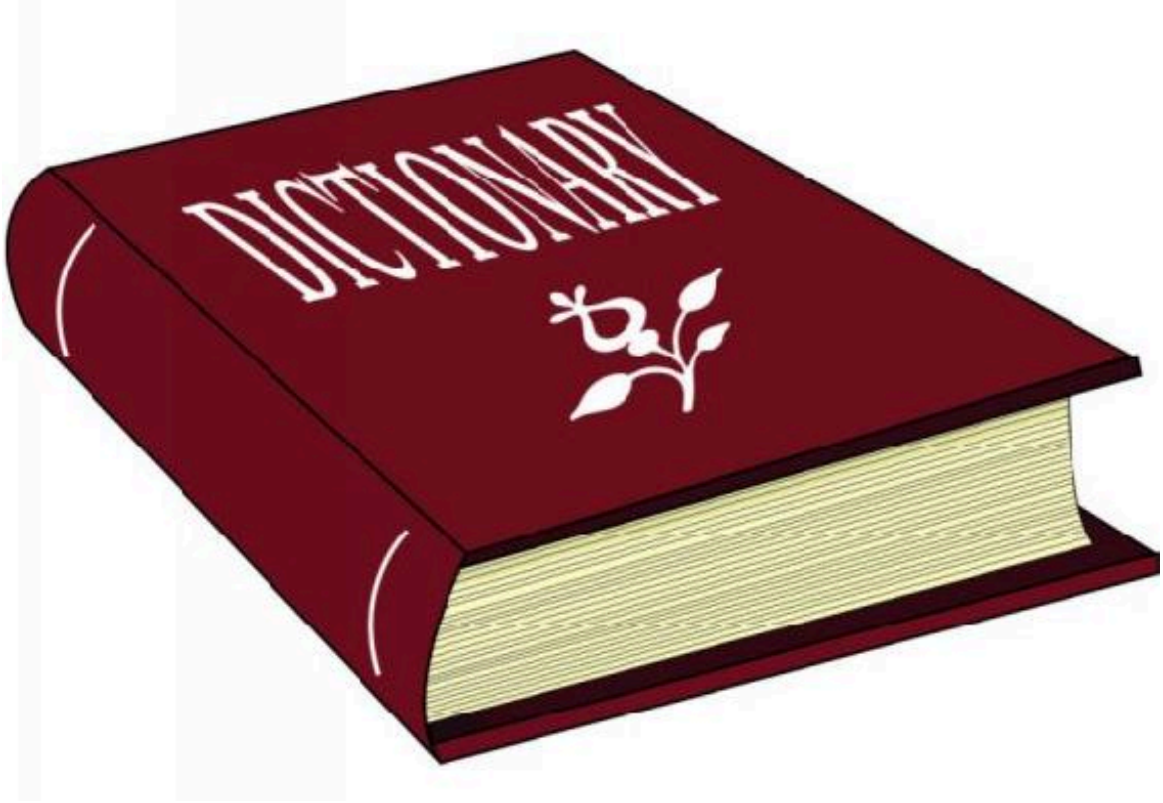
Nowadays people using mini hidden cameras that are disguised as a pen or watch, therefore you should always be very careful as you never know who is watching.

Brute force attack

In reality, there is no matter what your password is, as any password can be cracked using software JTR – John the Ripper, DenyHosts or Crain the Abel and much more. The only difference is that some weak passwords can be cracked in few minutes, and some strong passwords could take days if not weeks. I have explained before that using Back|Track OS, or Kali Linux, these tools are already built into those systems, and some of them just having a very user-friendly Graphical User Interface it is very easy to set it up, then let the software do the work until the password would be cracked. Again longer and more complex your password is, more difficult it is to be cracked. Then by the time, a JTR would crack your password you should change it so the software would have to start the process again. As I mentioned before every 20 days, your password should be modified, that used to be a recommended 30 days. However, the new recommended time for changing your password is 20 days. Still, there is no guarantee that your password will not be cracked. However, your chances will increase if you choose to have a very complex password.

Dictionary attack

Again the method is very similar to Brute force attack. However this time the attacker would use the dictionary list. There are build in files to operating systems such as Back||Track or the new version of Kali Linux, which can be loaded into a software and let that run until it finds the password.



Dictionary attacks can be implemented by using the same software sets as I explained before for Brute force attack, and again the most common ones are JTR – Jack the Ripper, Metasploit, or Crain the Abel. What it differ from a Brute force attack is that Dictionary attacks would start with the most common passwords first. Therefore it might have a faster result than having Brute force.

Rainbow Tables

This is a pre-computed for reverse engineering hash functions that are cryptographic for the goal in mind to crack multiple passwords.

This is more advanced, however overall this time the attacker would go for the database where all the passwords are kept. Imagine that there is a medium size company that has 1000 employees that are all required to have unique usernames, and passwords. Having that many usernames and passwords in the same place must be secured and hashed according to the Company policy defined by IT Security.

Advanced hackers wouldn't try to hack one password. Instead, they would try to steal them all. All usernames and passwords meaning not just an average employee, but the CEO, as well all the Finance, HR, Sales, Project Management, Business Continuity, IT Security, Service Management, Infrastructure Engineers, Technical as well Application Developers, IT Service Desk, Desktop Support and so on. All employees usernames and passwords can be taken by one go using Rainbow Tables. As you see there are more than a few passwords would be kept in the same place, they would

be hashed to be not visible to anyone, however having a rainbow table in place, it would recover plain text information to the attacker.

Keystroke logging

This technique can be implemented any many different ways, and the main purpose is to log everything that the victim would type into the computer possibly without even knowing it by the victim. The software can be installed by a Trojan so that once it would be on the victim's machine, it would activate itself and sending log files back to the attacker in a plain text format. Spyware has those functions too, and I already discussed on that topic. However, there are other methods to go about keystroke logging, and that would be using hardware.

Such hardware could be a USB stick that would begin to collect all the keystrokes. By capturing everything, the victim would type it would even include sensitive usernames and passwords. In large offices, the computers are often placed under the desk. Most people wouldn’t even bother to band down, and go below the desk to see if there might be some additional hardware are connected to the PC-s. However, this has been used before even with the Police, if they would investigate someone for monitoring purposes.

Social Engineering

I have explained some of the techniques and methods on how to find or crack passwords, however many people have an excellent skill set that would beat all the cracking methods, and that is Social Engineering. If you keep practicing, you can be so convincing, that certain people would believe whatever you want them to think. Manipulating people to achieve them doing thinks that they should never do can be very easy if you would impersonate employees. Imagine that you would call into an XYZ company and you would look ask to speak to the CEO. Most probably they would ask

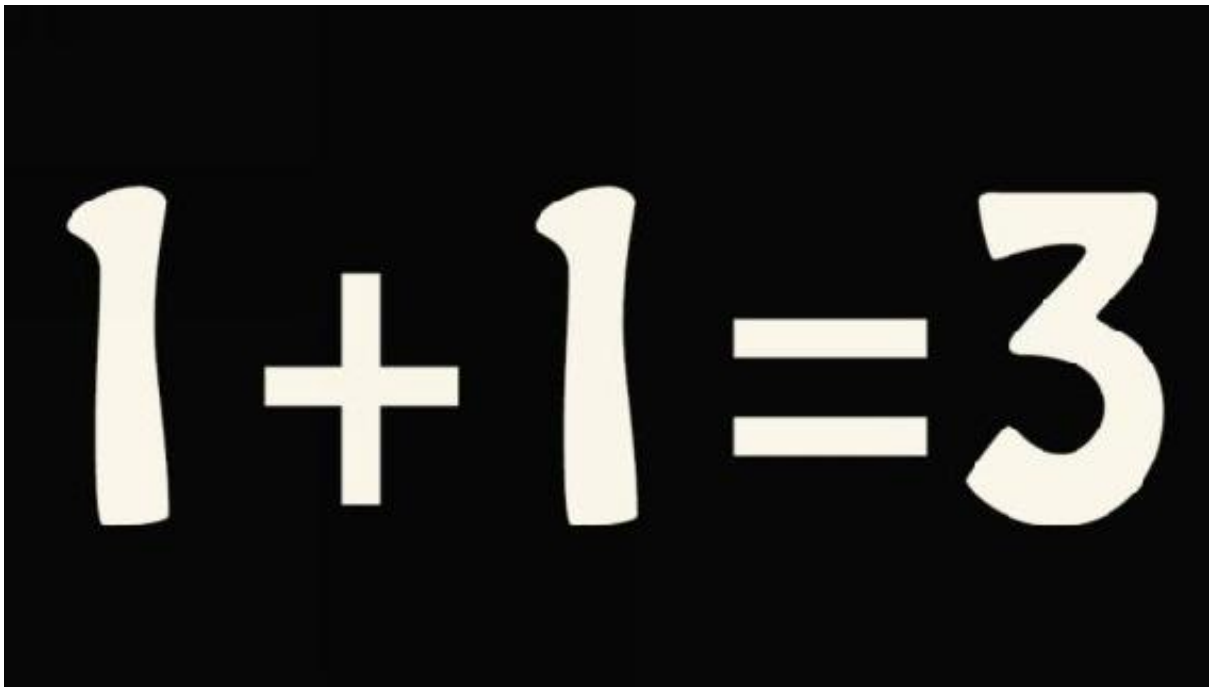
you who you are, so you could say that you are a brother or Sister. However, they would probably put you through to the CEO-s PA – Personal Assistant. But you should do first ask who you are talking to, so if they would state their name, for example, Peter from IT Helpdesk, you could take note of using it for future requirement. Once they would you through to the PA lets say called John, you should mention that they put you through to the wrong extension and hang up. Next, you could call back the IT Helpdesk, and say that you are a Jack, the PA to the CEO and already talked to Peter to change your password, but you still can not log in. And it's crucial as now you are in the middle of the meeting, and your presentation is required, so you would say to change the password quickly to something easy as the CEO already agrees that Peter made a mistake. The reality is that most people on the Helpdesk are afraid of the CEO, and they certainly wouldn't want to waste time and going through proper channels to change password for the PA of the CEO.

There are password policies in most places, and requirements exist to change an employee's password, however, once it comes to the Executives or Top management, unfortunately often the rules are bent. Most organizations take additional measurements for implementing secured password policies to follow. However, many new employees just started with the Company can be tricked to do certain things as they are still not sure of how the daily operation is running and might be afraid to ask questions regards to password change procedures for the CEO. There are many different ways that company employees can be manipulated. Therefore most organizations are severe on implementing better security policies to address these issues. Some places when it comes to training employees on how to deal with sensitive service requests such as password recovery, they would state that when it comes to trust and to question people, CEO-s or any highly ranked Employees must be challenged to prove their identities. Especially when some of these highly rated employees would be in the rush and frustrated, still they should be trained too, so if they wouldn't know the right answer to their security questions, their password will not be reset. Due to the password policy that requires employees to change their passwords in every 20 days, what I have experienced is that often when employees are returning from their Holiday,

they wouldn’t remember their passwords. So they would call IT Helpdesk to change or reset their password for something easy they can remember, then they would be able to log in, and change their password according to their requirements. Back to social engineering, there are multiple ways to manipulate employees. Therefore I would highly suggest that you do not share your password with anyone, especially be extra careful on the phone and it doesn’t matter who they claim they might be, following the company procedures you will never get into trouble.

Chapter 7 – Spoofing

Spoofing could de define as you would pretend someone or something that you are not. Faking your presents or your details to look like someone or something else. In simple terms, there isn't any other way I could describe spoofing. However, lets look at some examples, so you can understand how dangerous spoofing can be.



Voice Spoofing

It must have happened a few years back around 2012 when I got spoofed the first time, and I realized the potentials. What happened is that while I was at work sitting at my desk, beside another Security Engineer whose name is Ajay we have been working on a Business Continuity project for a Financial Organization. Business Continuity is paramount for Disaster recovery purposes, in case some disaster would happen and the company would lose the central head office, or worse all the buildings, the employees

would have a secured place to go to work. This place would be able to accommodate 100 people with PC-s and Phones ready to work. Sure this would not assist every employee. However, the management and selected people would be able to work. So Basically Ajay was configuring the VPN on the ASA (Virtual Private Network on a Cisco Firewall) while I was sitting beside him and creating a Visio Diagram for this new site, while I have realized that my mobile phone was vibrating in my pocket. When I looked at the phone, I already missed a call, so checked who I missed the call from, and it was a bit strange that I had a missed call from Ajay, in fact, I had two missed call from him already in the last 2 minutes. I looked at him, seeing that both his hands are on the keyboard since a long time, focusing on the project, so I just didn't understand what's happening. After a few seconds, I thought that he must have called me by mistake, so I just asked him:

-Ajay! Did you just call me?

He answered:

-I am busy dude, just give me a minute.

So I was now really confused. I couldn't wait any longer, as I saw on my mobile that he called me from his mobile as his name was on the phone. Because it only happened a few minutes ago, I thought that his phone is not locked and while in his pocket, I will keep on getting calls from him, and I just wanted to tell him to lock his phone at least even he is busy… So I started talking to him again…

-Ajay, your phone, keeps on calling me, where is your phone mate?

He then reached for his iPhone, when I saw with my own eyes that his phone was locked, but in the same second my phone was ringing again with his caller ID, so now I was a bit louder and saying:

-AJAY! You are calling me again man!

While he unlocked his phone, and we now both were looking at his phone, clearly see there is no dialing – he just said:

-I am not calling you! Pick it up, and see who it is!

So I picked it up, but the phone went dead.

Ajay and I were looking at each other thinking, how and what is going on, while I have realized that Roger from Telephony seems like laughing quietly, then I realized that some other engineers are laughing too. So now I have realized that is a good laugh for some of us, sure making fun of those trying to work hard, but I didn't agree, more like curious how it was done. I will not get into details now. However you have to understand that using Cisco Call Manager, newly called CUCM (Cisco Unified Call Manager) you can change the caller ID to anything you desire. There are many other platforms too that you can achieve the same result. However, this was done by the Call Manager.

I have talked about Phone Phreakers in Volume 1, and I have explained that back in the 80's old school hackers/phreakers used to play around making fun of people. This is a good laugh for sure, however spoofing voice by changing the caller ID, can be utilized by Black Hat hackers too. Imagine that you would receive a phone call, or a TXT message that saying that it was an Electric Company, asking you to call back due to necessary changes. So you would check the number, and you would see that is legit, but at the same time, they would be calling you again. So after you would pick up the telephone, they would explain that they have changed their Bank Details, therefore from now on you must make your monthly payments to their new account, and they didn't receive your payment yet. So, your current option is to pay what you own them, or they will shut down your electricity by the end of the day. You have time to make changes on your standard order. However, you must make the payment now to their new Bank Account that is only 45 dollars. The reality is that when Black Hat hackers spoofing the caller ID, you would believe they are legit and would make a payment. This is only one example. However, there are multiple ways to scam people with spoofing caller ID-s. Unfortunately, this technique is very efficient, and there are just too many victims out there, and it is tough to differentiate the good company from scammers, especially if they have an excellent social engineering skillset.

Spoofing comes in many other forms such as spoofing e-mails or websites, even a particular software can be fooled. However, the most common way

that is implemented is to spoof the caller ID.

Chapter 8 - Spamming

If you have a Yahoo mail or Gmail account you probably already have a spam folder. Spam is mainly spreader through e-mails, and if you do have a spam folder, you may as well open it and see for yourself what's in there.

Traditionally to advertise your products you can create an e-mail opt-in, so when people would visit your blog or website, visitors can sign up for future newsletters, or in case you have new products you might as well advertise it through e-mail to your list. This is legit. However, once it comes to Spam emails, they are not exactly legit e-mails. Moreover, they try to sell you something once you click on the links they would send you. Bad guys have realized, if they could automate this system and keep on sending e-mails to as many people as possible, they could probably make lots of money. At some point is true, however, what they do nowadays is that they would make your computer become an additional originator. So your computer would start to send e-mails too, and those e-mails would begin to reach everyone that are on your contact list. There are certain payloads,

which some of these emails, I should say spams are self-replicating themselves. Therefore your contacts would begin to forward those spams to their contacts and so on. As you see to stop these, can be tough, as the source is kept on changing, moreover, there are just too many, and you can not go and shut down everyone on the internet that has an e-mail address. Google. With their, Gmail has done some excellent job, as they have even additional filtering options for separating e-mails types, such as:

- Primary
- Social
- Promotions

Having those can be handy as for keep on looking at social website notifications all day long wouldn't be ideal. Many people think that opening such e-mails wouldn't hurt as they wouldn't buy anything anywhere. However, I am here to tell you, that you might be not buying anything but even just opening some of these spams can be just enough to trigger an additional forwarding to all your contacts. First I had had this issue when one of my close relatives sent me spam. In summary was:

, Hurry to reserve your Free flight ticket to the Canary Islands!''

But because he is my very close relatives, when reading the review, I have immediately called him. Surprise! He picked up saying:

-What's up? I am working, can we talk later, I will call you when I am off from work ok?

Hearing that he was at work, and don't have time even to talk, I was surprised that he was able to send me an e-mail, and I suspected something just not right. So I asked him:

-OK Fine, we can talk later, but did you send me an e-mail about free tickets to the Canary Islands?

He replied:

-What? I didn’t send anything to you, I don’t know what you were talking about, but I have to go now – will call you later.

We have discussed later and asked him to check his sent emails, but he said there was nothing there, no sent email to me or anyone, but some other people already called him as well asking him if these free tickets are genuine or not.

Then I asked him what did he do just before I called him, and he answered that he clicked like on a particular picture while he was visiting a web page of a well known social media site.

Spamming you it’s one thing, but once you become a spammer too, without even knowing about it, that’s not so great. Most people wouldn’t even bother calling you. Just think of you that you are sending some useless link again to click on. However, you as a sender wouldn’t even have any prove that you have ever sent these spams, as your assigned mailbox wouldn’t indicate that you ever sent any e-mail to anyone.

My final advise the following:

You do not click on spams, e-mails that you don’t know who they came from. I understand that some of them would have a very attempting summary, and some could be even sexual nature, but even opening such e-mails could compromise your details, and you might as well send the very same e-mail to all who are on your contact list, and that wouldn’t necessarily look professional.

Chapter 9 – Xmas Tree Attack

Before you would assume this type of attack could only around Christmas time, well, I can assure you it has nothing to do with the event no matter what religion you are looking at.

The details are more technical, therefore to implement Xmas Tree attacks, it is not recommended for beginners.

In Volume 2 - 17 Most tools every hacker should have, I have explained how you can craft and create any packet that you want using Scapy. As I explained in Volume 2 Scapy is indeed a very advanced packet manipulation tool, and you must have a good grasp of networking knowledge, how protocols work down to every single detail.

I have demonstrated by implementing few commands on how to use Scapy for Packet sniffing, furthermore also mentioned that Scapy could be utilized for creating a single unknown packet by changing any of its details such as:

- Any source address
- Any destination address

- Type of service
- We can create IPv4 Address or IPv6 Address
- Change any of the heather fields
- Replace the destination port number
- Modify the source port number

Additionally to craft a unique packet, Scapy also able to:

- Capture any Traffic
- Play or replay any traffic
- Scan for ports
- Discover networking devices

What it comes to an IP Packet, it would contain a heather as well a payload. The IP Heather itself would contain:

- Version – that would specify if it's an IPV4 or IPV6 packet
- IHL – Internet Header Lenght
- QOS – Quality of Service
- Length – The length of the packet
- ID – Identification Tag
- Fragment Offset
- TTL – Time to Live
- Protocol – This is a type of protocol such as TCP or UDP
- Checksum – This is for error detection

- Source IP
- Destination IP

Each has a flag that can be changed. Therefore would manipulate the network and once you would be ready to implement a Christmas Tree attack, you would want to change those flags by making it look like a Christmas tree. Simply by changing the flags to zeros and ones so the flag field would look like a Christmas tree.

Christmas tree attack would be used to certain networking devices at times where we wouldn't be exactly sure what type of devices are on the network. Each networking device would behave in a certain way, therefore due to certain responses, the attacker would be able to identify what kind of device is being targeted on the network.

Christmas Tree attacks could cause harm to networking devices in multiple ways. One of the most common ones is the targeted device would keep on rebooting itself in every one hour. For example, it would initiate a self-reboot at:

13:00, then 13:07 system back up and running ok

14:07 reboot again > 14:14 system back up and running ok

15:14 reboot again > 15:21 system back up and running ok

And so on and so forth…

This can be very annoying, as by basic troubleshooting an average engineer would assume that the network is fine, and it would seem that the issue would rely on hardware by having a defective device.

To avoid being attacked by a Christmas Tree types of attack, big business already invested into IPS-s Intrusion Prevention Systems that would help keep away fake crafted packets from Computer Networks.

Chapter 10 – Botnet

The name comes from the two words of roBOT and NETwork. We should categorize botnet as a type of malware. However, I have allocated a full chapter for this due to its power how dangerous can it be. What you have to understand is that once you have a botnet affected computer, it's called now a bot and it is under a third parties administration. You might think that you would be aware if your machine is affected.

However, I am here telling otherwise. The reality is there are millions of botnet affected computers, and other networking devices are out there, yet to identify any is very hard. As for the end-user, everything seems as it should be, and no issues with connecting to the internet, neither problems on the real PC, however, it might be already turned into a zombie also known as a bot.

More and more compromised computers become bots, larger and more powerful it can become the actual Botnet. What's happening is that each of

the zombie computers is now would call home that would be called a C&C Server – Command & Control. C&C is software. However, it would be on a Server. Therefore people refer to it as a C&C Server.

The attacker now would be able to control from the C&C Server all bots and do as he or she would wishes.

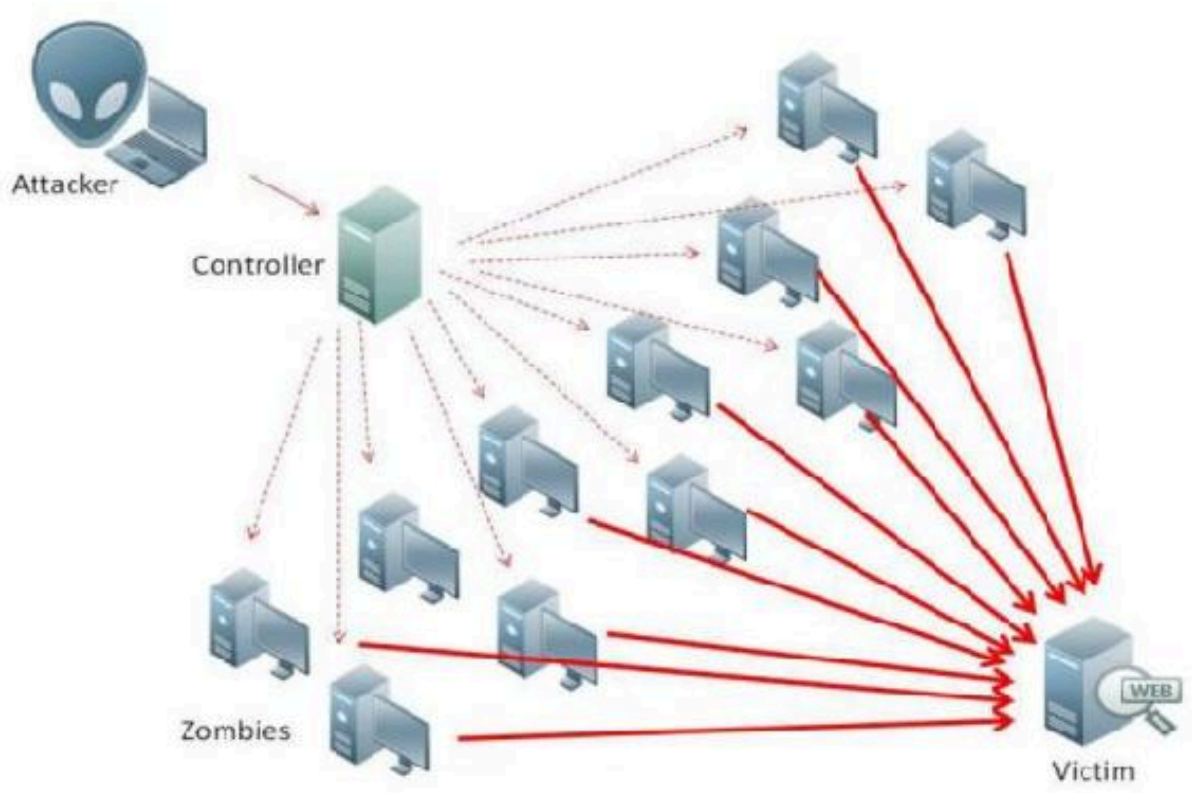
Origin of Botnet

A botnet is so powerful that doesn't necessarily require to be clicked on, but of course you can find those types of botnets too. The reality is that due to its malware type, Botnet can pick up from social networking sites, e-mails, free software downloads, youtube videos, free movie downloads. Similarly to Spyware, it can be obtained from many sources, and once your computer is affected, it can start to spread around to all your devices that might be on the same network as your modified device. For example, if you have a computer, a laptop, an X-Box, and a mobile phone on your home network and one of them is affected, believe me, all your devices will be affected. It can be self-spreader at some point, however, first when you would download a trusted free software from an untrusted source; it might contain a Botnet, that would be hidden under a Trojan type of virus. It might be in another form such as you receive a dodgy e-mail saying that you have been chosen and won x amount of money, so you must click on the link to claim your winning. Again, while you would click on that link, you wouldn't realize that the Trojan is already installing itself on your computer. Therefore it's very dangerous and nearly impossible to know if your PC might be already a Zombie. Additionally can be an infected media, that could be a USB Stick, or nowadays even cheap smartphones bought from China can contain Trojans that would spread around to other networking devices and create a robot network.

Relation between the bot and the C&C Server

Imagine that a torrent movie is effected with a Trojan that would contain a botnet, and there are around 2000 – 4000 people are downloading it every

day for the next three months, and eventually, those 300.000 computers would become a bot for a certain robot network. However you might think, how on Earth would all those bots connect to a C&C Server? First of all 300K computers to be on the same botnet is an average number. However, Cyber Security Experts have compromised Botnets previously that was large as 30 million zombie computers called BREDOLAB also was running on an alias as OFICLA. This was a Russian botnet. However it has been now compromised, but the reality is that we just don't know, at least can not be sure how many Botnets are out there.



So back to the victim's computer, once the botnet would install itself, called a BOT Binary, it would still have to look for a way to connect itself to the C&C Server to communicate with each other and exchange messages. BOT Binary can contain a hardcoded IP Address that would advertise out to the internet so the C&C Server would find it's bots. However, there are other methods too. Another common way would be that a particular Domain name is written into the BOT Binary that would be advertised out to find it's master C&C Server. Either way, once the Zombie computer registers

itself to the C&C Server, it will become a BOT officially, and the Robot Network Army begins to grow.

Botnet purpose

There are good intentions too for some who creates and uses such Botnets. However, there are very few as we know yet. And what I heard is that in certain countries certain websites are blocked therefore a few communities are using Botnets to access the information that their government wouldn't allow them to view according to their law.

The reality is that Botnets are used mainly by the bad guys, but to be more specific, large Underworld Cyber Criminal Organizations.

Similarly to Spyware, once your computer becomes a bot, it could forward all sensitive information to its master – C&C Server that might be usernames, passwords, bank account information, however, the primary purpose of the Botnets are deeper than that.

Some people would only build Botnets so that they could sell it to Cyber Criminals, and larger the botnet is more value it has. Of course, there are certain botnets would contain only bots from the US, or from Europe so those would be a little cheaper. However, large Botnets that has bots all over the worlds in different continents are more expensive. A botnet that would contain a C&C Server and 50-100 bots would be sold between $200 - 800 Dollars, however, it all depends on the locations of the bots too. Now taking this further, large Cyber Criminals have multiple botnets, each would contain 10K + zombie computers, and they would letting them out for an hourly fee, or daily fee. Again it would depend on the requirements, as well the quantity of the bots, and their location, but an average price would be for 5000 bots with C&C Server for 1 hour is around $100, or $1000/Day.

When it comes to a botnet of 5000 bots, you have to understand that not all 5000 zombie computers can be used at the same time, as some of them might be turned off. However, I wanted you to understand the pricing when it comes to a marketplace.

Again back to a purpose of the botnets, some organizations would use it to create a DDoS attack (Distributed Denial of Service) against a particular

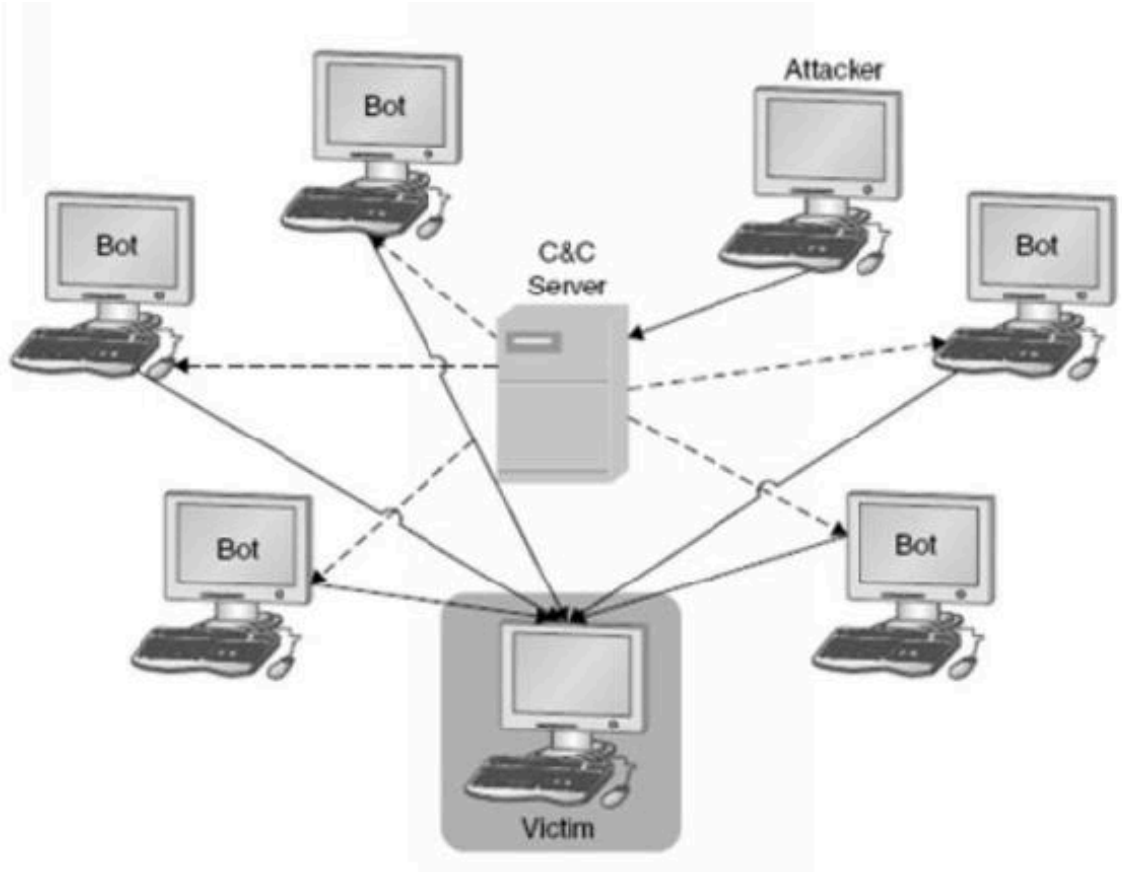
company, perhaps against their competition, or it could be a revenge of an ex-employee. Either way, botnets can be used for attacks, but more and more it used for financial gain, and that is Bitcoin mining.

Bitcoin mining is very popular, however to mine Bitcoin you must have a huge amount of CPU power combined. Therefore large botnets can be a perfect for this exercise. This process is also known as Silent Bitcoin Mining. However, this must be controlled accurately as for Bitcoin mining all the bots would use 100% CPU. Therefore they would control that so the victims wouldn't realize that silently their computer (bot) is mining Bitcoin.

Who is the behind the C&C Server?

As I mentioned, all the bots are Centralized and controlled by the C&C Server. Due to the centralized coordination to compromise such robot network the source must be identified and caught. The reality is that such Bot-master would always be very careful and would probably only log into the C&C Server if it's fully Secured. Of course, there is nothing more than guaranteed then a multi-layered network called TOR.

TOR network would allow the BOT master to be anonymous. Therefore it would remove all traces of his or her identity, that would result in the BOT master to be untraceable.



How to Avoid your computer to become a Zombie?

The answer is simple – back to basics! Do not download software from untrusted sources, even if the software is free you must make sure that you are getting it from the trusted source. Downloading torrents like movies, music, or video games, I would recommend you do not do it, as for the potentials for those items might be affected is very high.

E-mails that advertising things that are too good to be true, DO NOT OPEN them, period.

Your Computer should not remember your username and password/s either. Also in case you buy a new laptop, of desktop computer, you must change the passwords. Furthermore, just be careful, and being reasonable with the information presented to you. For example that you have won 1Million Dollar, so all you have to do is to click on the link to claim it if you didn't even play anywhere, how would you win anything right!? – So again, do

not click on anything that you are unsure of, especially for weird programs that would supposedly help you achieving thinks like hack into someone's Facebook Account and thinks like that.

You must purchase an Antivirus and update it regularly; second is you should install a Firewall even if it's virtual, still would help you identify if you are affected. Next, to that, you must always run the latest operating system especially if you have Windows. Normally they do upgrades within their software as they have now found a vulnerability within the previous Operating system, therefore upgrade required to patch those vulnerabilities.

Chapter 11 – SQL Injection

Before I begin to talk about code injection, you should understand the meaning of the SQL Server.

Think about Facebook for a moment, and when you log in at first and create a new account. Facebook, in fact, any other large platform would require you to provide bare minimum details such as your:

- First Name
- Surname
- Date of Birth
- Username
- Password

Then all these details would be stored in an organized manner. Next, you would begin to add additional information about yourself such as your relationship status, then add Family members, as well friends. Again all

these details are kept in the background away from the users and would all be kept in the DBMS – Database Management System.

DBMS would refer to as a collection of programs that would help you to access the database, also manipulate individual data, and help you to represent your data. Facebook is a lot more than just keep your data, as it would also be stored as a storage for your video contents, images, messages, and so on. However anytime when you log in to Facebook using the right username and password, your details would be coming up first as well everything that is related to you. Therefore Relational DBMS would be used most times, as also is the most popular. Such systems are:

- MySQL
- Microsoft SQL
- Oracle Server

As I mentioned, these are the most traditional relational DBMS servers on the market.

SQL – Structured Query Language, and this would be defined as a standard language when it comes to relational DBMS-s.

So what is SQL Injection you might ask? Well, this type of attack is on the top 5 lists when it comes to web application attack, mainly because it is super easy to perform. Commonly would be done on login screens where you should provide your username and password. The attacker first would type a SQL quote instead of a username and press enter. This would cause an issue behind in the SQL Server, therefore would cause an error if the website wasn't properly built. The point is the attacker now would know there is a SQL Server behind the web application and so now would begin to implement the code injection. The code that would be injected it can be a simple code such as that I would ask for the SQP Server to allow me to log in without a password. Again back to Facebook if I would confront and interact with the login page, and I would use your username and your password instead of mine, Facebook would load your profile, not mine. So

my point is that once you are interacting with the login page by typing something in there, you are communicating with the SQL Server at the back end. While you are talking to the back end of the SQL Server, you are interacting with the code that has been written. Therefore you might as well type your code in the Login field instead of your username or password to Create a SQL Injection.

Unfortunately, bad job of coding could leave open doors for the bad guys and surely they would take advantage of it. The problem is that if someone would be able to log in as an admin, without a password, they could have potentially had access to everything behind the database. Imagine that you would have access to everyone's messages within Facebook that would be crazy right? Facebook might not be the worse, however, if someone would break into a Bank's SQL Database, and have access to everyone's Bank account that would be an entirely different story.

Programmers when writing the code, before completion must have a double, even triple check the web application making sure they have tidy up properly the back end so the bad guys wouldn't be able to implement SQL Injection.

Chapter 12 - Distributed Denial of Service

Before we get into the nitty-gritty details of complexity, let's just take a step back and think about what a Denial of Service means.

Denial of Service

Also, know as DOS, in fact, most IT pro would refer to as DOS. Denial of Service can be explained in multiple ways, however, in a simple put, this is an event when something or someone would prevent an individual system to operate.

Before moving on to any technical details, please take a moment and think about how much could it cost for someone to cause a Denial of Service to a certain Organization? My hint is this: Do not overcomplicate it, and forget about any technical implementation! Also, try to come up with the cheapest ever that could be to cause such event to a small sized company let's say no more than 500 people.

OK, I assume that you have thought about it, so let me elaborate on this. Some of you might think, that you need large systems, and enormous power

of CPU capacity, even internet connection and so on… Some of you, in fact, most people think to cause a Denial of Service to an average company, the minimum that also could be enough is a laptop, so when thinking about a second-hand laptop, you may say a hundred bucks right?

What if I would tell you otherwise? What if I say 50cents would be just enough. I know it sounds weird and may think that is impossible, but think again. Imagine that an evil guy would walk into a public payphone, then dial a company or a large building reception saying there is a bomb in the building, then walk away. Unfortunately, thinks like these does happen all the time all over the word. As you see, there is no technical knowledge required, neither a laptop to cause a Denial of Service. This example would probably cause an average company a great fortune. Think about what would be a standard procedure in case of receiving a bomb threat. First, a full building evacuation, next to the police, or some bomb squad have to go through the whole building making sure there is no threat. I would say the minimum downtime for those employees while they would be unable to work at least 3 hours. 3 hours of an outage when an average employee would be on wages of $10 per hour could cost a company of 500 people at least $15K loss. Not to mention that particular work, and other losses would be too. In case there were a guest or future clients who would experience such event, would also consider doing business. Of course, some employees would resign right then, resulting the company to spend on ads for vacancies, additional interview processes and training for new staff and so on.

When most people think of a Denial of Service, begin to wonder about black hat hackers and huge technical knowledge, but in reality, it could be done with a simple phone call, costing less than a dollar in 10 seconds.

DoS in a Digital world

Denial of Service is happening all the time, however, let’s look at the history of DoS in the news. By the end of 90’s and the beginning of the 21st Century Denial of Service was all over the news. Back then this is a new type of attack had to be in the headline, and companies were that got hit were happily explained what experience they have gone through. Slowly by

getting close to 2010 these types of attacks, seemed to be dropped, or at least we do not hear them as much in the news as we used to. Why is that? Companies have realized that by keeping on getting hacked or having their websites, or web services down is not so good for their reputation. Instead of willingly admitting that they have been a victim of a denial of service attack, they would only deny it, and state those are false statements from whatever who is spreading the word about it. Now think about an insurance company that would be kept on getting hacked, and their website almost never usable. Why would you insure yourself or any of your belongings with them if they can't even insure themselves? Well, you wouldn't. Because back in the day was cool to talk about it, now it is changed, as even to mention that a company has been hacked or their web services have been taken down, would exhibit weakness in their Security Infrastructure.

Denial of service can be done and caused in multiple ways, but most commonly the result would be the same, and that is to stop the website from functioning.

Very common is when there is a known vulnerability in certain systems software that would be require patching. Large companies would announce this issues publically, and for those having a contract with them, and anyone really who are registered on their e-mail lists, and happy to receive newsletters about the latest and greatest. So basically no one keeps away from the bad guys to receive the same news as those who would require implementing patching. IN the production environment, these could have high importance. However, most patching would require system reboots, and those changes should take place out of hours.

So when you think about average company standards and Change management procedures, such as planning the change and approvals, could take days, if not weeks. However, if some exceptional Infrastructure Managers can convince the business that these changes would require completion ASAP, they might just be able to complete patching vulnerabilities in the same day as they would receive the news. Threating vulnerability patching as an emergency change is indeed a good idea, however, if you can only implement the required patching at the evening, that might be already late. When you think about black hat hackers, they

don’t need any approval or change management meetings to attend, all they have to do is take down your website. Therefore DoS attacks are very common. In fact, if you want to watch them DoS attacks in life, you can go ahead and visit Norse: http://map.norsecorp.com/#/

Norse has more than 8 million sensors around the globe, so they have been able to create a map of live attacks.

The reason for DOS?

Why would anyone ever implement a Denial of Service? The answer is to deny a particular service yes, but why? In Volume 1 of my book have explained the History of hacking and that show up with certain achievements were very popular back in the days. It was all about fame so that hackers can be recognized from one another. There was, of course, the fun side of it too for some. However, those days are nearly over. Don’t get me wrong, as I do know that people like these exist, and they will never go away. However, the time has moved on. As time moved on hackers have grown up too, and those have historically been involved in significant hacking and implementing attacks like DoS, or even DDoS, are now have a different lifestyle. Some may have become White hat hacker, or a Security Expert is having their company or helping out large corporations, or government agencies as a Cyber Security Consultant. When it comes to a Financial gain, DoS attacks might be helpful for some, and let me explain the reason for it. As of 2017, there are 5 to 10 companies that are producing high-quality mobile phones around the globe. There are more than that, but I am looking at the five most common brands out there. So imagine that one of them could take out the rest of them by keeping on causing DoS for their web services. This is what we call Cyberwar. This is already happening since years, in fact, it always existed, but now it’s hitting the digital world.

Banks, and other financial organizations, in fact, countries keep on attacking each other, and if you follow the news, you might have heard that some countries even lost their internet connection for hours. Traditional DoS attack can take down a website yes, but take down the whole country, and then no one knows who did it? This is the world we leave in, so we just better accept it as is.

DDoS

What it stands for is Distributed Denial of Service, but technically called DDOS., pronounced as deedos.

I didn't get into so much detail when I explained about DoS, so now let me elaborate on it. I have mentioned that a DoS attack would cause of preventing a certain service or website to function, and I mentioned one common technique that hackers can use. However, there is another way that DoS or even DDoS is very famous about it.

I have been visiting certain websites that had issues just before days like Black Friday, or even Christmas period. Matters such as the site is unreachable. This is happening simply because the website has so many visitors at the same time, that the site would eventually crash. As for Black Friday, when everything has a price decrease, you might find many websites will not be able to function after a while due to a high number of visitors. However Black hat hackers would take down sites, using the very similar technique of a vast number of visits at the same time.

TCP SYN Flood attack

I have explained in Volume 2 how TCP works and why it's so important to understand to be a great white hat hacker or Security Engineer. To visit a website, certain protocol stacks help us allowing the connection. One of the most common is a TCP – Transmission Control Protocol. TCP uses a 3way handshake to establish a connection between the client and the server. In the standard TCP connection when the end user types into the browser a website address, it would initiate a SYN packet, called a synchronize request. Next, the Server would answer with the SYN-ACK packet, meaning the synchronized packet was acknowledged. As for the third part, the client should send an ACK packet, recognizing that the server was responding, and now the 3way handshake would be completed and the communication would be established so that the end user would see the website on the screen.

When a black hat hacker would implement a TCP SYN flood attack in DDoS format, only the SYN packet would be sent to the server from multiple hosts simultaneously, and the server would keep on running out of space by remembering to wait for the ACK packet from each client that originally initiated the SYN requests.

Ping of death

Another way to cause DDoS attack is using echo requests by the ping utility. Again I have explained before how to use ping and what is it for, but the remind you, ping is formally used to check the reachability of a certain device on the network. Once a client would initiate a ping also known as an echo request to a certain server, there would be an echo reply from the server. When it comes to DDoS, there would be multiple clients that would initiate the echo requests simultaneously causing the server to stop functioning.

I have mentioned for both examples the word: multiple clients; this would mean that the black hat hacker would use a BOTNET, robot network to do

either TCP SYN Flood attack or Ping of Death. Cyber criminals would probably use both attacks methods at the same time, even addition types, in the form of multiple BOTNET-s.

Protection against DDoS

First, let me tell you that DDoS using various BOTNET-s can take down any website, it's only a matter of when rather than can it be done.

Implementing Rate limiting against TCP SYN Flood attack is a bare minimum, and echo request/reply should be turned off to protect against the Ping of Death. There is off course should be IPS, and IDS systems should be in place as well Firewalls, and large organizations this is a must to provide an always-on web service.

Chapter 13 – Worms & Virus types

Worms

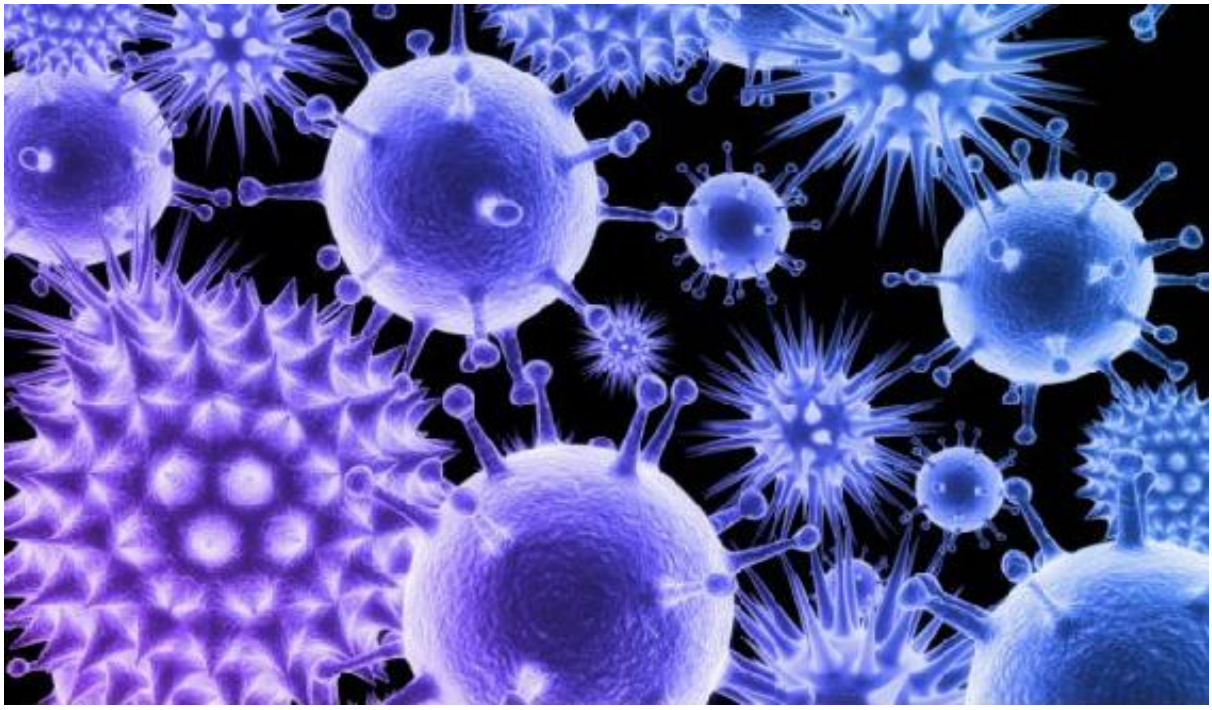
There are many different virus types, in fact, there are thousands are identified every single day, however, when it comes to worms, they seem to be a little different to standard types of viruses.

One of the reasons that worms are different then viruses is because they don't need to be executed my a human end user. Only they would spread between networking devices by having them on, and connected to each other. They are self-replicated. Therefore worms can infect large organizations, and they can spread all over the internet too. Some types of worms can self-replicate themselves so fast that they can spread over thousands of computers just under few hours. There were some old types of worms that they have been spreading so quickly on the network that eventually created so much traffic that they have brought down the system.

However most of them are silent types, and they are tough to identify, furthermore, once they have been determined on certain computers, by the time you would try to clean them up they would be spreading over to other computers, therefore giving us a hard time. Intrusion prevention systems and intrusion detection systems can help us identify and prevent them from getting on our systems.

Virus

When it comes to viruses, they would require being turned on by clicking on to be executed. Computer viruses are very similar to real viruses that humans could catch, and often a virus could be speeded from one person to another. This is what a Virus could do, however, once I virus would be executed, it would begin to infect other software, systems too. Although there are different types of viruses, could achieve different results. Some of them are similar to worms and silent types, therefore tough to identify them.



Some could cause simply slow down the performance of the computer, while the end user would blame the actual computer, however, in reality, the virus is who is responsible. Some other viruses would sit on the computer doing nothing but wait for a reboot. Once the computer would turn back on,

the virus would execute itself, causing the boot process not to start, and so the computer wouldn't turn back on. Again the end user wouldn't know what happened, as while the computer was working there was no problem whatsoever, but when trying to proceed with a reboot, it will not occur. Let me expand on some well-known viruses with further details.

Macro

Also known as Melissa Virus, was introduced itself just at the end of the 20th Century. Melissa was spreading through an e-mail that had an important document attached. What happened is that people had to click on the attachment, and that triggered to send the same e-mail to everyone in your contact list. Therefore it was spread all over in less than a week was causing more than 70 million dollars of damage. Even that millions of computers were affected, the primary harm that caused was only on companies Servers.

I LOVE YOU

The I love you Virus was another similar worm to Macro, and the technique was very similar too. Again people with curiosity were affected mostly due to the Subtitle of the e-mail: I love you. Additionally, there was an attachment that was named: Love letter for you.

Of course millions of people just had to click on the attachment as they all believed they might have a secret admirer. Unfortunately, it was another surprise instead, and that is every single file on the computer has renamed itself as: I love you, and all data become useless, including pictures, videos, music, and files at the same time. It was originated from the Philippines in 2000, infected more than 40 million computers in less than three days, causing more than 10 billion dollars of damage.

Mebroot rootkit

This piece of a virus was downloading itself without any visibility, therefore the owner did not even know there was any issue with the computer. What its job was to overwrite the computer's boot record that was telling the computer to connect to a botnet called Torpig. Torpig is also known as Sinowal or Anserin, and its primary job is to use the technique called the man in the browser. What the man in the browser does is sees everything that is being typed into the computer, therefore capturing every single keystroke, then forwarding those to botmaster. Torpig has stolen nearly half a million of credit card information just in less than a year.

SQL Slammer

This was another very dangerous computer worm that caused DoS Denial of Service as many ISP-s routers just couldn't handle it's traffic, causing many countries to lose internet outage.

It has infected more than 70000 victims in less than 10 minutes. It was mainly affecting Microsoft SQL Servers. Apparently, there was a patch released a half year earlier. Still, many companies didn't find the time to implement it.

As I mentioned before, there are thousands of new viruses are identified in every day. Therefore I could go on and on about computer viruses. What you have to get from this is that each computer worm or computer virus has a different purpose, and to identify them can take time, and often only able to do it when the harm already happened.

What you can do to protect yourself is a bare minimum to have an up to date antivirus, frequently updated. Also, try to make sure that your computer is always running the latest operating system for better security against known vulnerabilities.

Chapter 14 – Logic Bombs

When you think about a real bomb, you have to understand there are so many different kinds out there and each type is or can be triggered in a different way to explode it. When it comes to a logic bomb, it works somewhat in similar ways than real bombs, however, to find a logic bomb on a computer it might be very difficult, often impossible to do so. A logic bomb instead of exploding like real bombs, it would execute itself on a special event, or some the more advanced types of several incidents.

An example could be that once installed on a computer system; it could cause to shut down itself exactly one week after the installation.

Other types of logic bombs might be programmed to be triggered for other reasons such as for a certain time. For example, when the clock hits 1 pm on every Wednesday, initiate a reboot. However when you would look at

the logs, you wouldn't see anything or any human interaction that could have caused such event, therefore yet again, it would act very silently.

Logic bombs could be something like that would spread on the system and only would trigger itself if it would meet a specific brand, that has a specific model number, that would have a particular part number is online and functioning at speed rate of x.

I have provided some very specific examples of a particular target, in a very specific way, however, logic bombs could cause other harms too such as:

-Rebooting servers,

-Deleting certain files

-Encrypting certain documents

-Destroying important files

Logic bombs are waiting to be triggered, and some might be waiting for a given moment. However, some have been written in the past to expect for the next system reload to explode itself.

In the past, it has been identified few times, which ex-employees have been involved in creating such logic bombs, because they have been dismissed, and so they wanted to commit an act of revenge on the company they have worked for by damaging their systems, resulting in a company a financial loss.

Chapter 15 – Trojans horse

You might be familiar with the story of Troy. According to the Green mythology what happened is the Greeks have tried to concur the city Troy for many years. However, it seems to be impossible. Then the Greeks have built a wooden horse having their best soldiers hiding inside and left it outside of the gates of Troy, making it appear as a gift. Once the wooden horse was inside Troy, the soldiers have been able to sneak inside of the city of Troy, and they were able to let in other soldiers from the inside of the gates.

When it comes to a computer virus called Trojan horse, also known as Trojan the concepts are very similar. A Trojan virus is very famous of being hidden inside a certain program, or file that might be a computer game, or

software that is available for free download. Once the victim would download the piece of software to the computer, the Trojan would execute itself begin to do its purpose. As you remember the wooden horse created by the Greeks, the primary objective was not to be inside and destroy but allowing others inside first. Therefore the Trojan's first move is often to disable the firewall or antivirus or often both of their functionality. Once the firewall is disabled, there would be backdoors created, and certain vulnerabilities would begin to become open for any intruders.

Some Trojan viruses are typically has been written for creating backdoors and letting in other malware such as spyware, or adware. However it all depends on the original purpose of the attacker, but most times, it is to have full control over the computer.

Having full control, could potentially making the victim's computer to join to a botnet, or could cause even a Crypto-locker, and demand payment.

When I had a Trojan virus on my timeworn laptop around 2004, it was such a pain. I had no choice but to reinstall a new operating system, and I have lost all my files due to it's earlier version of the virus, that had a purpose of destroying data. Black hat hackers and Cybercriminals have realized that having fun and utterly destroying computers has no meaning. Therefore the game has changed. Most Trojan nowadays has a purpose of some financial gain.

A later version of Trojan horse virus that was popular is having a Scareware installed on the computer. Scareware is real to scare victims, by popup messages, such as:

Your computer in danger, click here to scan for viruses!

So by clicking on a popup that seems like part of a Windows operating system, a fake antivirus would pop up, and begin to scan the computer for viruses. These are so fake that once you have experienced this, you just know that as it scans your computer in 5-10 seconds, then showing you lots of different kind of viruses that you should quarantine. However, when you try to isolate those bad viruses, you would be prompted to pay for the antivirus software such as 40 to 100 dollars one-time fee. Normally what

happens is that once you would make a payment, you would be prompted to download the full software that would contain even more backdoors, such as adware or spyware, or even keystroke logger, but certainly not an excellent antivirus. As it would go on, you would be kept on prompted for additional issues on the computer. Examples are that you have a Trojan and that to be removed would require you to buy another software that is specifically for Trojan virus removal. It would be a never ending story. Therefore the best way often is to re-install the operating system, and next time be extra careful with drive-by-downloads, or anything that could be coming from an untrusted source. As I mentioned these types aren't visible as much as they used to be as most Trojans, you wouldn't even be aware that you have downloaded, and they would be most possibly connect computers for robot networks.

Researchers show that over 10% of all computers in the world are attached to a botnet, and it was due to Trojan virus that started the actual infection on those machines.

How to remove Trojan viruses

Removing viruses can be done, however Trojans might have infected some of the legit software-s that have been previously installed on the computer, therefore might be tough to do so. In fact, you can never be 100% sure that you have removed all the viruses from your computer. However, you can give it a go with a good Antivirus. What you have to do when you begin is to reboot your computer and start it in safe mode. It all depends on your operating system that you are running, however, once you are in safe mode, you may proceed to execute an antivirus by doing a full scan. Once complete, you should do a test and see if your computer gets any faster. Also, try multitasking with a lot better performance, and then you should do another additional full scan making sure there are no more viruses. As I mentioned before, Trojans can be a real pain, and you might never be able to fully remove them, therefore as I suggested earlier your best option might be to re-install a brand new operating system.

Chapter 16 - Ransomware

Ransomware also is known as Locky, or Cryptolocker is a malicious software that blocks access to your computer while asking for a ransom to be paid to unlock your screen. There are different types out there, some might be threatening you that all your files are now encrypted and will be lost if you would not pay, yet another would threaten you to pay, or all your files will be uploaded publicly.

It has begun to grow internationally in 2012, however by 2013 the number of victims has doubled, making Ransomware a real nightmare. The attackers are asking to pay between $200 to 500 dollars on an average, in exchange for a system decryption. The problem is that when you would receive a lockdown screen, additionally you would have a clock that would count backward. The timer is another technique for the purpose of creating an urgency for the victims. When you think about that you might need a file

on your system that you want to access within a week, even if it weren't urgent, now it would suddenly become a major one. One of my best friends had it first in 2014, and the attackers have asked him to pay 400 dollars within 48 hours, or the files will be destroyed within his computer. He is a Graphic Designer, and working from home. What he does is taking on certain jobs, such as drawing comic books, or even designing logos and delivering those projects on the internet. He has been working on a project to complete a short comic book that was required to have 20+ pages, and he was very close to finish when he got a ransomware that has blocked his computer. Unfortunately, he had no backups, and the delivery date was about to do. Even he would have been able to re-deliver it again; it would have been taken him weeks, not to mention that he must have had another computer as the ransomware infected machine was useless. He paid of course, not like any option he could have chosen from, however after the payment he has been told that they will only decrypt half of the files on his machine unless he pays another $200. Being in a desperate situation, the hackers have made him pay again. However, after his files have been decrypted the outcome still wasn’t what he expected. The way he explained to me, is that some of his files have not been decoded correctly and they were corrupted, and some of them were useless anymore. Fortunately, the actual project he was working on had no infection, and he was able to deliver it just before the deadline. When he called me and explained what happened, I was speechless. Well not actually, instead I kept on asking him, why didn’t he call me, but the way he has described the situation to me, I knew right then that I had not much that I could have helped really.

You might think it’s not a big deal, however, when you consider that these black hat hackers are ruthless and only interested in financial gains, you know that it’s not right. Many people working from home, and they make a living by doing so. Therefore taken advantages on these, and steal their wages are just not fair. Not enough that cyber criminals are damaging intellectual property and threatening innocent hard working people by asking for ransom, they even take this further.

Chapter 17 - WannaCry

Another new type of ransomware called WannaCry has hit the world just in May 2017. Attackers have used a very same or somewhat similar technique as any other ransomware. However, it was different than traditional locky. This time it seemed that was released worldwide affecting 99 countries just in less than five days. However, 3 weeks after the cyber attack the new report showed that more than 150 countries had victims. More than 70000 cases have been reported from all over the world.

In the US one of the most famous Delivery company FedEx have been affected, as well Homeland Security adviser has added that several US government services also have been affected.

In China, more than 30000 companies have been affected, including government agencies, schools, and hospitals.

In the UK, mainly the NHS – National Health Services were affected. Close to 50 organizations have been hit with ransomware, in a result of GP-s and hospitals were unable to use their computers. As I live in the UK and I have friends who are working in the NHS, they have told me that not every NHS organization has been hit, also wasn't spreading around as at many other

companies. The fact is that NHS has so many networks, it would be impossible to add them together. This, of course, was one of the reasons NHS got lucky as one of my friend said they had not been affected even a slightest. I also know that NHS is not exactly a company that after profit, therefore they have got the latest tech neither like to spend money for network security or raising the salary for people's wages in the IT department. The problem with unusable computers in hospitals, and GP-s are simple. When you get sick and making a phone call to book an appointment, the receptionists would take your details, and their in-house system would help to find the earliest date available. Unfortunately, the computers were down, and receptionists had to get back to paper/pen style, and taking details like the old times. The problem with these is that no one can tell when the next available appointment is. Additionally, the phone lines got busier as each of the phone calls was taking a lot longer. Shortly a day after the cyber attack has started, they have announced in various news channels, and radios the following:

Please do not call the NHS, unless is an emergency situation!

When you think about calling the hospital or even your local GP for an appointment, but they would tell you that is not a case of urgency, so you have to wait, it's certainly not your dream. Turned out that was nobodies wish. There was a little chaos. Additionally to appointments, there were people with scheduled surgery dates, and if you know how long that typically takes, then you are aware that some people have to wait a year + sometimes to have such appointment. What happened with many people has they had their operation, or surgery canceled, as all the important details would require for the operation, wasn't available anymore as they were unable to get into the computers.

While I was working for a Financial Organization at work, we have increased the Firewall reports, and begin to take a closer look at them. Of course, no one has mentioned anything like it, but I tell you the truth; I was scared for days. I mean who want to face with a locked screen that is demanding for $300 worth of Bitcoin!

Every single issue that was reported, we have been taking a look as never before. For example, helpdesk has indicated that one of the wireless networks has slowed down! We were all over the place looking at the possible issues that could have been, however, turned out that only one of the Access Point had to be bounced as it wasn't registered to the WLAN (Wireless LAN) Controller. Then another incident has been raised that our website wasn't available, but actually, it's not hosted by us, and they had a scheduled maintenance for that. In the end, we had no effect of any ransomware whatsoever. However, it has kept us on out toes.

In France, the car company called Renault has been effected, and some of their factories had to be suspended manufacturing car parts while they have replaced their computers.

In Spain one of the biggest Telecom company called Telefonica has been hit with ransomware, affecting more than 1000 computers. However, they have replaced them quickly to keep the company up and to run.

In India close to 20 systems have been hit and most of were state police computers.

Russia has reported over 1000 computers that have been affected by WannaCry ransomware, and according to Kaspersky Lab, Russia has infected the most from any other countries.

When you closely look at this incident, you may realize that most places the computers were hit were all running some outdated Windows Operating System that wasn't upgraded or patched accordingly. Therefore I would recommend to always keep your computer up to date with the latest operating system running. Additionally, make sure that you have an active Antivirus, frequently updated.

Who is behind the attack? I have my theory, and I am not blaming a particular country's government like some news channels. In my opinion, it was more like an individual organization. However I will not dare to mention who and for what reason might have caused this Cyberattack, as even my theory is correct about who might have done it, I am still not sure the exact reason what is their plan with this. According to the Bitcoin wallet, there were only just a little more then 300 payments have been made to the attackers' portfolio, profiting only around $100K, meaning it wasn't for a profit. Shortly we might be able to figure it out exactly who did it and for what reason, but for now keep safe and be aware.

Conclusion

Thank you for purchasing this book.

I hope this title was able to get you started on your pursuit to be an Ethical Hacker also known as Penetration Tester.

The next step is to simply take extra measurements and start protecting yourself implementing a stronger password policy, having an up to date Antivirus and an always on Firewall.

Once you begin to apply this methods, you will gain additional knowledge and will help you empower to become an Ethical Hacker.

By now you probably realized that I have explained more then 17 hacking methods, and you understand the facts that are thousands of new viruses are identified every day.

I hope this content helps to prepare you for our current digital world and to avoid being hacked.

Lastly, if you enjoyed the book, please take time to share your thoughts and post a review. It’d be highly appreciated!